INTERNATIONAL AND COMPARATIVE BUSINESS LAW AND PUBLIC POLICY | 04

BLOCKCHAIN AND PRIVATE INTERNATIONAL LAW

Edited by
Andrea Bonomi,
Matthias Lehmann,
Shaheeza Lalani

UNIL | Université de Lausanne

BRILL | NIJHOFF

Blockchain and Private International Law

International and Comparative Business Law and Public Policy

Series Editors

Andrea Bonomi, *University of Lausanne*
Damiano Canapa, *University of Lausanne*
Andreas R. Ziegler, *University of Lausanne*

Editorial Board

Thomas Cottier, *World Trade Institute & University of Ottawa*
Shaheeza Lalani, *University of Lausanne*
Eva Lein, *University of Lausanne*
Francesco Maiani, *University of Lausanne*
Vincent Martenet, *University of Lausanne*
Andreas Ziegler, *University of Lausanne*

VOLUME 4

The titles published in this series are listed at *brill.com/blpp*

Blockchain and Private International Law

Edited by

Andrea Bonomi, Matthias Lehmann and Shaheeza Lalani

BRILL | NIJHOFF

LEIDEN | BOSTON

This is an open access title distributed under the terms of the CC BY-NC-ND 4.0 license, which permits any non-commercial use, distribution, and reproduction in any medium, provided no alterations are made and the original author(s) and source are credited. Further information and the complete license text can be found at https://creativecommons.org/licenses/by-nc-nd/4.0/

The terms of the CC license apply only to the original material. The use of material from other sources (indicated by a reference) such as diagrams, illustrations, photos and text samples may require further permission from the respective copyright holder.

The open access publication of this book has been published with the support of the Swiss National Science Foundation.

Library of Congress Cataloging-in-Publication Data

Names: Bonomi, Andrea, 1964- editor. | Lehmann, Matthias, 1972- editor. | Lalani, Shaheeza, editor.
Title: Blockchain and private international law / Andrea Bonomi, Matthias Lehmann, and Shaheeza Lalani.
Description: Leiden ; Boston : Brill/Nijhoff, 2023. | Series: International and comparative business law and public policy, 2667-3495 ; vol.4 | Includes index. | Identifiers: LCCN 2023030936 (print) | LCCN 2023030937 (ebook) | ISBN 9789004514843 (hardback) | ISBN 9789004514850 (ebook)
Subjects: LCSH: Blockchains (Databases)–Law and legislation. | Conflict of laws–Technology transfer. | Technology and law.
Classification: LCC K564.C6 B58 2023 (print) | LCC K564.C6 (ebook) | DDC 343.09/99–dc23/eng/20230808
LC record available at https://lccn.loc.gov/2023030936
LC ebook record available at https://lccn.loc.gov/2023030937

Typeface for the Latin, Greek, and Cyrillic scripts: "Brill". See and download: brill.com/brill-typeface.

ISSN 2667-3495
ISBN 978-90-04-51484-3 (hardback)
ISBN 978-90-04-51485-0 (e-book)
DOI 10.1163/9789004514850

Copyright 2023 by Andrea Bonomi, Matthias Lehmann and Shaheeza Lalani. Published by Koninklijke Brill NV, Leiden, The Netherlands.
Koninklijke Brill NV incorporates the imprints Brill, Brill Nijhoff, Brill Schöningh, Brill Fink, Brill mentis, Brill Wageningen Academic, Vandenhoeck & Ruprecht, Böhlau and V&R unipress.
Koninklijke Brill NV reserves the right to protect this publication against unauthorized use.

This book is printed on acid-free paper and produced in a sustainable manner.

Contents

List of Illustrations ix
Notes on Contributors x

Introduction: The Blockchain as a Challenge to Traditional Private International Law 1
Andrea Bonomi, Matthias Lehmann and Shaheeza Lalani

1 The Role and Prospects of Private International Law Harmonisation in the Area of DLT 10
Gérardine Goh Escolar

PART 1
Fundamental Questions

2 Technical Description of DLT for Conflicts Lawyers 51
Tetsuo Morishita

3 Should Crypto-Asset Regulation Be Technology-Neutral? 66
Bruno Mathis

4 Is Bitcoin out of Reach for Private International Law? 81
David Sindres

5 Proprietary Rights in Digital Assets and the Conflict of Laws 101
Christiane Wendehorst

6 The Good, the Bad and the Ugly: The Private International Law, the Crypto Transactions and the Pseudonyms 128
Anne-Grace Kleczewski

PART 2
Blockchain Assets and Conflict of Laws: General Issues

7 Taxonomy and Characterisation of Crypto Assets in Private International Law 157
Felix Krysa

8 Crypto Assets and Decentralised Ledgers: Does Situs Actually Matter? 209
Amy Held

9 The Law Applicable to Crypto Assets: What Policy Choices Are Ahead of Us? 259
Burcu Yüksel Ripley and Florian Heindler

10 The Law Applicable to Digital Representations of Off-chain Assets 285
Emeric Prévost

11 Cryptocurrencies and Conflict of Laws 314
Francesca C. Villata

PART 3
Specific Blockchain Assets & Legal Relations

12 The Law(s) Applicable to Central Bank Digital Currencies 351
Caroline Kleiner

13 The Law Applicable to Stablecoins 372
Matthias Lehmann and Hannes Meyle

14 The Tort Law Applicable to the Protection of Crypto Assets 399
Tobias Lutzi

15 International Insolvency Law and Cryptocurrencies 417
Giovanni Maria Nori and Matteo Girolametti

16 The Law Governing Secured Transactions in Digital Assets 456
Matthias Haentjens and Matthias Lehmann

17 Do Smart Contracts Need New Conflict-of-Laws Rules? 479
Mehdi El Harrak

18 Blockchain-based Negotiable Instruments: with Particular Reference to Bills of Lading and Investment Securities 494
Koji Takahashi

19 Conflict of Laws and the Use of Distributed Ledger Technology in Derivatives Markets 529
Gregory Chartier

PART 4
Blockchain & Dispute Resolution

20 Blockchain Dispute Resolution for Decentralized Autonomous Organizations: The Rise of Decentralized Autonomous Justice 549
Florence Guillaume and Sven Riva

21 Recognition and Enforcement of the Outcome of Blockchain-Based Dispute Resolution 642
Pietro Ortolani

PART 5
National Reports

22 Conflict of Laws and Tokens in Swiss Private International Law 673
Pascal Favrod-Coune and Kévin Belet

23 Blockchain and Private International Law – The Perspective of the United States of America 709
Frank Emmert

24 A German Approach: *Lex Supervisionis Registri* and Subordinate Connecting Factors 727
Felix M. Wilke

25 DLT and PIL from the Perspective of Liechtenstein 754
Francesco A. Schurr and Angelika Layr

26 Blockchain and Japanese Private International Law 765
Tetsuo Morishita

Index 791

Illustrations

Figures

2.1 Mechanism of blockchain 53
2.2 Diagram of bitcoin transactions 61
2.3 Diagram of securities transactions 62
6.1 Screenshot of a random public address on Ethereum, as displayed on Etherscan 132
8.1 Christie's standard conditions of sale (London version), clause 9 221
8.2 Gemini user agreement, governing law and dispute resolution provisions 222
8.3 Coinbase user agreement, clause 13.21 223
18.1 Inter-operability of digital negotiable instruments 509
18.2 Issuance and trading of security tokens 511
18.3 Trading on a distributed ledger 512
18.4 Post-trade clearing and settlement on a distributed ledger 513

Tables

1.1 Overview of connecting factors 17
5.1 Categories of assets 103

Notes on Contributors

Kévin Belet
holds a Bachelor of Law and a Master of Law and Economics from the University of Lausanne where he is a PhD candidate and completed a Certificate of Advanced Studies in International Business Disputes. He is currently a trainee lawyer in a law firm in Lausanne.

Andrea Bonomi
holds a law degree (Padua), a PhD in Comparative Law (Innsbruck) and a PhD in Private International Law (Bologna). He is a Professor of Private International Law and Comparative Law at the University of Lausanne and the former Director of the Centre for Comparative, European and International Law of the Lausanne University. He has been a visiting professor at several universities and was invited, in 2007, to teach a Special Course at The Hague Academy of International Law. Member of the Swiss delegation at the Hague Conference of Private International Law, he chaired the Special Commission on the Law Applicable to Maintenance Obligations and is the Rapporteur of the Hague Protocol on the Law Applicable to Maintenance Obligations of 23 November 2007. Co-editor of the *Yearbook of Private International Law*, Prof. Bonomi is the author and editor of more than 200 books and articles on private international law and comparative law topics. He is also a Member of the European Group of Private International Law (GEDIP), an Associate Member of the International Academy of Comparative Law, and a former Member of the Arbitration Court of the Swiss Chambers' Arbitration Institution (now the Swiss Arbitration Centre).

Gregory Chartier
is a qualified lawyer in England and Wales and a Senior Associate in the London office of Clifford Chance. He specialises in advising on cross-border structured finance transactions, including advising clients in respect of structuring and documenting OTC derivative transactions in all asset classes and repo and securities lending transactions. This includes advising on the use of smart contracts and DLT in relation to derivative, repo and securities lending transactions.

Mehdi El Harrak
holds a Doctor of Laws from the Sorbonne Law School. He is a lecturer in law at the University of Lausanne with fields of expertise in Comparative law, Private International Law, and International Trade Law. His PhD thesis describes offset contracts in an international trade context. He used an interdisciplinary

approach based on his previous position as legal adviser with Orano SA, a multinational nuclear fuel cycle company, to analyse strategic and military transactions. He has been lecturing in Bucharest at the Franco-Romanian College of Law, at SciencesPo Paris, at ESSEC Business School and at the Burgundy School of Business. He regularly speaks at international conferences and seminars to share his expertise and research. Since 2017, while pursuing postdoctoral research at the University of Lausanne, Dr El Harrak specialised in Financial Contracts, Blockchain and FinTech.

Frank Emmert
is a tenured professor at Indiana University Robert H. McKinney School of Law in Indianapolis and the Director of its Center for International and Comparative Law. He teaches International Business Transactions, International Commercial Arbitration, Blockchain and Digital Currency Law, Consumer Law, World Trade Law, International Investment Law, as well as European Union Law, and has published more than 100 books and articles in these areas of law. Prof. Emmert has taught courses for credit at Cardozo, Tulane, Temple, Rutgers, IU Bloomington, and Stanford in the USA, St. Gallen and Basel in Switzerland, as well as Alexandria, American University Central Asia, Amsterdam, Cairo, Charles University Prague, College of Europe, Guadalajara, Sheffield, Strasbourg, Tallinn, Tec de Monterrey, URJC Madrid, USEK Lebanon, and several other universities. He is the co-founder and chairman of the Council on International Law and Politics, co-founder of the Blockchain Law Alliance, Member of the Silicon Valley Arbitration & Mediation Center, and a Fellow of the Chartered Institute of Arbitrators in London.

Pascal Favrod-Coune
holds a Bachelor of Law and a Master of Law (*summa cum laude*, Commune d'Ecublens Award), and a PhD in Law (*summa cum laude*, Walther Hug Award and Charles-Philippe Mercier Award) from the University of Lausanne, and an LL.M. from the London School of Economics. While writing his PhD thesis on the legal aspects of crowdfunding, he was a visiting scholar at the University of California in Berkeley and the Max Planck Institute for Comparative and International Private Law in Hamburg. He is currently a lecturer in Finance, Law and Digitalisation at the University of Lausanne, an associate of the Centre for Blockchain Technologies of the University College London, and is practising as an attorney at law in Geneva.

Matteo Girolametti
is *magistrato ordinario in tirocinio* at the *Tribunale di Milano*, appointed by D.M. 2.3.2021. He previously was a trainee lawyer at DDPV Studio Legale in Rome

(2016–2020), mainly dealing with antitrust issues, and a trainee judge at the Italian Supreme Court (2017–2018). He graduated from the LL.M. Programme in International Business Law at the University of Lausanne in 2022 and graduated in law from *Università degli studi di Camerino* (2016) where he defended his thesis on predatory pricing between abuse of a dominant position and attempt to monopolise.

Gérardine Goh Escolar
is Deputy Secretary General of the Hague Conference on Private International Law (HCCH). Concurrently, she is Head of the HCCH's International Commercial, Digital and Financial Law Division, with primary responsibility over the normative projects on Central Bank Digital Currencies (CBDCs), Digital Assets and Tokens, and the Digital Economy, as well as the HCCH 1985 Trusts and 2006 Securities Conventions, and the HCCH 2015 Principles on Choice of Law in International Commercial Contracts. Dr Goh Escolar was previously in practice, acting as counsel, advocate and consultant in international litigation and arbitration proceedings, first with a specialist international law boutique, and then with a top-tier global law firm headquartered in Amsterdam (the Netherlands). Prior to that, she was Legal Advisor to the President of the Iran-United States Claims Tribunal, and principal legal officer in the chambers of a Judge at the International Court of Justice, the principal judicial organ of the United Nations. She has also served as legal officer with the federal government of Germany, in-house counsel at a technology company, and vice-president of external relations at an information technology startup. Dr Goh Escolar is full Professor (Adjunct) at the Faculty of Law, National University of Singapore, and has extensive academic experience over two decades.

Florence Guillaume
is a Full Professor of Civil and Private International Law at the Faculty of Law of the University of Neuchâtel (Switzerland). Her research and publications cover a wide array of topics, including international corporate law, international business litigation, international intermediated securities law, national and international succession law, international trust disputes, and legal issues of digitalisation. She founded in 2020 the LexTech Institute, which is an academic center dedicated to research and training in digital technologies. Before entering academics, Prof. Guillaume practised as a lawyer at the Geneva Bar and the Zurich Bar. She also worked as a Deputy to the Head of the Private International Law Department at the Swiss Federal Ministry of Justice.

Matthias Haentjens
is, since 2012, a Full Professor of Law at Leiden Law School, where he currently holds the chair for Civil Law. Prof. Haentjens obtained a Master degree in

Greek and Latin at the University of Amsterdam. He obtained his PhD in law at the University of Amsterdam and has been a visiting scholar at Université de Paris II (Panthéon-Assas), Harvard Law School, New York University School of Law and Ghent University. Prof. Haentjens has been a member of the Expert Group on Securities and Claims at the European Commission, of the Consultative Working Group on Investment Management at ESMA, and a consultant to the World Bank. He works part time as an attorney (*advocaat*) at De Brauw Blackstone Westbroek and since 2020, he has been a member of the Working Group at UNIDROIT in its Digital Assets and Private Law initiative.

Florian Heindler
is an Assistant Professor at Sigmund Freud University, Austria. He obtained Masters in Law and in Slavonic Language Studies as well as a PhD in Law. In addition to his academic position, he is legal counsel to an Austrian bank. He has several publications in the fields of private international law, comparative law and Austrian private law. He is an Associate Member of the International Academy of Comparative Law and Chairperson of the Interdisciplinary Association of Comparative and Private International Law. He has been a visiting scholar at the Swiss Institute of Comparative Law.

Amy Held
was called to the Bar of England and Wales in 2019 and has been a University Assistant at the University of Vienna since 2020. She has maintained an academic specialisation in the private law aspects of cryptoassets and decentralised ledger technologies from both national English law and private international law perspectives since 2017, with Masters research analysing the private law consequences arising from the adoption of decentralised ledger technology in the financial markets infrastructure, and doctoral research exploring the harmonisation or unification of national substantive property laws as part of a proposed comprehensive private international law regime for decentralised assets. She continues to publish and lecture widely on these and related issues in both the academic and practitioner contexts, with a particular emphasis on property law. In 2022, she was a National Rapporteur for the IACL World Congress Study on cryptocurrencies for England and Wales/UK, and was involved with UNIDROIT's current projects on Digital Assets and on Effective Enforcement as part of her residency in Rome as a UNIDROIT Scholar.

Anne-Grace Kleczewski
works as legal counsel at Bonnard Lawson (Switzerland). She is specialised in technology law, and advises clients with respect to blockchain-based projects. She was part of the corporate law department at a major Belgian law firm and a legal advisor with the Swiss Institute of Comparative Law. She is a doctoral

student at the University of Louvain-la-Neuve (Belgium), at the Centre for Interdisciplinary Research on Business Law (CRIDES). Her thesis focuses on the liability of online platforms for infringements committed by their users. She approaches the problem from a European, Swiss and American law perspective. She has been involved in research projects relating to the regulation of the collaborative economy as well as more generally online platforms and artificial intelligence. She has published relevant academic papers on these issues, as well as in various legal fields, including taxation.

Caroline Kleiner
is a Full Professor at the University of Paris Cité (formerly University Paris V, René Descartes), where she teaches Private International Law, International Banking Law, Banking Law, International Business Law and International Contracts. She holds a doctoral degree from the University of Paris 1 Panthéon-Sorbonne and her thesis was related to currency in Private International Law relationships. She publishes extensively on International Banking Law, International Litigation and Private International Law in French, English and German. She has acted as an arbitrator and legal expert in international cases involving banking and financial law.

Felix Krysa
is a University Assistant at the Department of European, International and Comparative Law, University of Vienna (Austria). His research areas are in the field of private international law of crypto assets and European private international law. In his PhD research at the University of Bonn (Germany), he focuses on the private international law of data protection with special consideration of the General Data Protection Regulation.

Shaheeza Lalani
is the Executive Director of the LL.M. Programme at the University of Lausanne and was the Founding Director of two other postgraduate programs in Switzerland. She holds a Bachelor of Arts Honours degree in History and French Studies from Queen's University (Canada), a Master of Science in Public Policy and Public Administration from the London School of Economics (United Kingdom), a Bachelor of Laws and Bachelor of Civil Law from McGill University (Canada), and a PhD in Law from the University of Lausanne, where she won the Faculty Prize for her thesis in Private International Law. She is a barrister & solicitor, admitted to the Law Society of British Columbia and has taught courses at the Universities of Fribourg, Bern, Lausanne and Paris. Previously Senior Legal Counsel with the Swiss Chambers' Arbitration Institution

and Legal Counsel to the Swiss Institute of Comparative Law, Dr Lalani has worked as an Assistant Legal Officer with The Hague Conference on Private International Law (HCCH) and has authored and edited several publications on international law and arbitration.

Angelika Layr
is a Legal Officer at the "Office for Financial Market Innovation and Digitalisation" (SFID) at the Government of Liechtenstein as well as a PhD Candidate at the University of Lucerne. Previously, she was a Research Assistant at the Universities of Lucerne and Liechtenstein. She graduated in law from the Johannes Kepler University Linz and holds a Bachelor of Science (BSc), as well as an Executive Master of Laws (LL.M.) in Company, Foundations and Trust Law from the University of Liechtenstein. Prior to her studies, she worked for an international corporation in supply chain management. During her studies, she has been a research assistant at the Chair of Company, Foundations and Trust Law, at the University of Liechtenstein. In addition, she has gained practical experience in a tax firm, as well as in a trust company. In October and November 2021, she was invited as a visiting scholar to UNIDROIT Rome, where she advanced her research on digital assets and digital transactions.

Matthias Lehmann
is a Full Professor at the University of Vienna, where he holds the Chair for Private, Private International, Civil, and Comparative Law, and a Rotating Professor of European and Comparative Law at Radboud University of Nijmegen. Previously, he was a full professor at the Universities of Halle-Wittenberg and Bonn. He holds doctoral degrees from the University of Jena and Columbia University as well as a *Habilitation* (professorial thesis in Germany) from the University of Bayreuth. His main interest is in cross-border financial law and regulation as well as dispute resolution. He is a member of the International Academy of Comparative Law, of the Council of the European Law Institute (ELI) and of the Academic Board of the European Banking Institute (EBI), Prof. Lehmann has participated in the European Commission's Expert Group on Conflict of Laws Regarding Securities and Claims, in the UK Financial Market Law Committee's working group on distributed ledger technology, and in the UNIDROIT Working Group on Digital Assets and Private Law. He is regularly teaching as a guest professor at the Sorbonne Université, the Université de Fribourg, the Université de Lausanne, and the Universidad Pablo de Olavide in Spain. Prof. Lehmann has been a visiting scholar at the London School of Economics and Political Science, Oxford University and Stanford University.

Tobias Lutzi
is a junior professor at the University of Augsburg. He has studied law in Cologne, Paris, and as a Rhodes Scholar in Oxford, where he completed his doctoral thesis in 2018. He is the author of 'Private International Law Online' (OUP 2020), the general editor of conflictoflaws.net, and a chair of the Young Research Network of the European Association of Private International Law.

Bruno Mathis
is an associate researcher with ESSEC Business School's European Centre of Law & Economics (CEDE) in France and a freelance consultant. He developed his career in the software industry and consultancy services dedicated to investment banking, with a focus on compliance systems and procedures. He is conducting research in digital law, more specifically on blockchain and digital transformation of justice. He is also involved in a cross-disciplinary project in computer-sciences and law, led by the University of Nîmes, to extract knowledge from judicial data with machine-learning. He is a graduate of École Supérieure de Commerce de Paris.

Hannes Meyle
is a lawyer with Walder Wyss. His areas of expertise include legal issues relating to e-commerce and IT security, data protection law, intellectual property, competition and antitrust law, and private international law. He studied at the University of Geneva and at the Ludwig-Maximilians-University in Munich. During his legal clerkship with the Higher Regional Court of Munich, he worked with a leading international commercial law firm in Munich. He also worked with the Chair of International Private Law and Comparative Law at the University of Geneva, where he received his doctorate in 2020 (*summa cum laude*) on a topic related to international private law.

Tetsuo Morishita
is a professor of law at Sophia University, Japan. He worked for The Sumitomo Bank, Limited (Japan) from 1989 to 1999. In April 1999, he moved to Sophia University, where he has been teaching International Business Law, Banking and Finance law, and Negotiation. He has served as a member of various meetings at the Japanese Financial Services Agency, such as the Payments Council on Financial Innovation (2016–), the Study Group on the Virtual Currency Exchanges Services (2018), the Working Group on Capital Market Regulation of the Financial System Council (2020–).

Giovanni Maria Nori
is a Research Fellow in Commercial and Industrial Law at *Università degli studi di Urbino Carlo Bo*. He completed his PhD degree in Economic Law in

the Department of Management and Law of the *Università Politecnica delle Marche* and defended his thesis on ICSID Arbitration and the International Protection of Foreign Investments. He graduated in law from the *Università degli studi di Camerino* (2015) and defended his thesis entitled "*Il contratto di rete come strumento per l'organizzazione e l'internazionalizzazione dell'impresa*". He is admitted to the Italian Bar and is an Assistant Professor of Commercial Law at the *Università degli studi di Camerino*.

Pietro Ortolani
is a Full Professor of Digital Conflict Resolution at Radboud University in the Netherlands. He holds a law degree from the University of Pisa and a PhD in arbitration from LUISS Guido Carli University, Rome. Before joining Radboud University, he was a Senior Research Fellow at the Max Planck Institute Luxembourg for Procedural Law, a Research Associate at the University of Pisa and a Law Research Associate at Queen Mary, University of London. He is admitted to the Bar in Italy and also works as a practitioner, mainly in the field of arbitration. He has experience in both *ad hoc* and institutional arbitration. He has acted as an expert for the European Parliament and the European Commission.

Emeric Prévost
is currently University Assistant at the University of Vienna (Austria) and lecturer at Meiji University (Tokyo, Japan), where he teaches International Business Law. He also teaches International Financial Law for the International Law LL.M. diploma of the University Paris Cité (France). He has also acted as expert for the Council of Europe and the European Commission on SLAPP-related issues. His PhD research at the University of Strasbourg (France) and the University of Turin (Italy) focuses on financial disintermediation and private international law methodology. He is also admitted to the French bar and shortly practised in Paris, advising clients on a wide array of banking and financial law regulatory issues.

Sven Riva
is a PhD student in Private International Law at the Faculty of Law of the University of Neuchâtel (Switzerland) and a member of the LexTech Institute. His thesis deals with the international legal scope of decentralised autonomous organizations (DAOs) with a focus on international corporate law, a field in which he specialised in writing his Master Thesis and as a member of an international group of experts that drafted a Model Law for DAOs. He has a general interest in financial market law, in particular in fintech regulation, blockchain law, and decentralised finance (DeFi). He has written on the application of the rules of private international law in the areas of digital integrity, artificial intelligence, and international judicial assistance.

Francesco A. Schurr
is a Professor of Law, Chair of Italian Private Law and Comparative Law, at the Innsbruck University Law School as well as Head of the Institute for Italian Law. Since 2009, he has been a Professor of Law, Chair for Company, Foundations and Trust Law at the University of Liechtenstein, as well as Director of the LL.M. program in Company, Foundations and Trust Law. Since 2011, he has been a Co-Director of the Centre for the conclusion of his habilitation in 2004. Francesco has been appointed frequently as a visiting and adjunct Professor, *e.g.* at the University of Padova, the University of Bolzano, the Victoria University Wellington (New Zealand). In his numerous publications he has focused on issues of private law in general, contract law, consumer protection law, foundations and trust law, company law as well as European and private international law. Francesco is admitted to the legal profession as Avvocato in Bolzano (Italy) and as Rechtsanwalt in Munich (Germany). In 2021, he was appointed as Judge at "The Court for Trusts and Fiduciary Relations" of the Republic of San Marino.

David Sindres
is Agrégé des Facultés de Droit and Professor of Private Law at the University of Angers (France), where he teaches Private International Law, International Trade Law, Contract Law, Tort Law and Comparative Law. He has also taught Private International Law at the Sorbonne Law School and at Sciences Po Paris. His main field of research is private international law.

Koji Takahashi
is a Professor at the Doshisha University Law School in Kyoto, Japan. After completing his LL.B. and LL.M. degrees in Kyoto and LL.M. and PhD degrees in London, he started his full-time career in England, first as a researcher at the Institute of Maritime Law of Southampton University and then as a lecturer at the Birmingham University. He has taught and researched in various areas of English law and after returning to Japan, focused largely on private international law, Japanese law and comparative law. Prof. Takahashi has been on the editorial board of the Journal of Private International Law since 2005. He launched his personal blog 'Blockchain, Cryptocurrency, Crypto-assets and the Law' (https://cryptocurrencylaw.blogspot.com) in 2015 and has since published a number of articles in that field.

Francesca C. Villata
is a Full Professor of International Law at the University of Milan, where she teaches Private International Law, International Contracts and Arbitration, International Financial Markets Law. She has been a member of several legislative panels, such as the Expert group on conflict of laws regarding securities

and claims (European Commission, DG Justice), the DLT Governing Law and Jurisdiction Working Group (Financial Market Law Committee, London) and the Working-group for the implementation of private international law rules on civil partnerships (Italian Ministry of Justice). Moreover, Professor Villata serves as Managing Editor of the *Rivista di diritto internazionale privato e processuale* and, since 2013, has been working on several DG Justice funded projects in the area of EU private international law, as coordinator and/or member (EFFORTS, IC2BE, Diginlaw, EUFams I and II, EUPillar, Insolvency, Suxreg). Finally, she is a member of the EU Law Committee of the Bar Council of Milan.

Christiane Wendehorst
is a Professor of Civil Law at the University of Vienna. She is, among other things, a founding member, immediate past President (2017–2021) and since 2022, Scientific Director of the European Law Institute (ELI), as well as Co-Head of the Department of Innovation and Digitalisation in Law. She is a member of the Bioethics Commission at the Austrian Federal Chancellery and Vice President of the Austrian Jurists' Association (ÖJT). She is President of the Humanities and Social Sciences Division of the Austrian Academy of Sciences (ÖAW) for the term 2022–2027. She is also an elected member of the Academia Europea (AE), the International Academy for Comparative Law (IACL) and the American Law Institute (ALI). Before moving to Vienna, she held professorships in Göttingen (1999–2008) and Greifswald (1998–99) and was Managing Director of the Sino-German Institute of Legal Studies (2000–2008). Her current research focuses on the legal aspects of digitalisation and she has acted as an expert on issues such as digital content, the Internet of Things, artificial intelligence and the data economy, *e.g.* for the European Commission, the European Parliament, the German Federal Government, the ELI and the ALI.

Felix M. Wilke
is a Senior Lecturer at the University of Bayreuth (Germany), where he works at the Chair for Civil Law, Private International Law and Comparative Law. The University of Bayreuth awarded him his doctoral degree for a comparative study of the general issues of private international law in the European Union. Dr Wilke also holds a Master's degree in Law from the University of Michigan, USA. He has been teaching and publishing in German and English about/on all areas of Private International Law (jurisdiction, applicable law, recognition and enforcement) as well as on topics of substantive private law.

Burcu Yüksel Ripley
is a Senior Lecturer and the Director of the Centre for Commercial Law at the University of Aberdeen. She obtained her LL.B. and PhD in Private International Law from Turkey, and her LL.M. in International and Comparative

Business Law from England. Before joining the University of Aberdeen, she worked at the Department of Private International Law of the Ankara University Law Faculty. She also practised law, enrolled with the Ankara Bar Association, and worked at the Export Credit Bank of Turkey (Turk Eximbank). She has several publications in the fields of private international law, international trade and finance law, international payments, international commercial law and dispute resolution, and digitalisation. She has been involved in international collaborative research projects and appointed by courts in the UK and Turkey to give expert opinion evidence on matters involving a foreign element. She is a Constructing a Digital Environment Fellow of the Digital Environment Expert Network of the UK Natural Environment Research Council.

Introduction: The Blockchain as a Challenge to Traditional Private International Law

Andrea Bonomi, Matthias Lehmann and Shaheeza Lalani

1 Blockchain as a Global Information Register

Since it made its first appearance in 2008, the blockchain has been on everyone's lips. Over the last couple of years, cryptocurrencies like Bitcoin or Ether, gained exponentially in value before the crisis of the crypto industry that began in November 2022 (also termed the "crypto winter"). Yet, the technology underpinning the blockchain – known as distributed ledger technology (DLT) – lends itself for other purposes as well, for instance to safely transfer data, to measure the usage of services or objects or to control the authenticity of documents. Tokens recorded on the blockchain may even confer voting rights in collective entities known as "Decentralized Autonomous Organizations" (DAOs). On the horizon, new forms of dispute resolution are emerging, which combine the use of DLT with artificial intelligence (AI). There may be other potential applications which one cannot yet fathom.

But what is the blockchain? The Chapter by Tetsuo Morishita provides a detailed description, so a few words will suffice here. At its heart, the blockchain is the first truly global register for the safe recording and transfer of information. Its particularity – and the major innovation – lies in the fact that the information is not stored in a single place but on a network of nodes distributed all over the world – hence the expression distributed ledger technology, or DLT.[1] These nodes keep an identical copy of the register, which they continuously update after having validated any changes to it. Once a block of new information has been added to the chain, it can no longer be altered; apart from a few exceptions, the ledger is immutable. In essense, the blockchain is a synchronised and secure information register that is kept all over the world. The second generation of blockchains allow for the execution of more complex operations rather than just the mere transfer of information, which has given rise to so-called decentralised apps, such as smart contracts. Contracts

1 Although the blockchain is not the only application of DLT, it is by far the most relevant one. For this reason, and because the term is much more evocative than 'distributed ledger technology', it has been chosen for this book.

© ANDREA BONOMI ET AL., 2023 | DOI:10.1163/9789004514850_002
This is an open access chapter distributed under the terms of the CC BY-NC-ND 4.0 license.

can thus be made or performed without the need or possibility of human intervention.

All of these characteristics give rise to tremendous challenges in Private International Law (PIL). But, is the blockchain out of reach for PIL? In Chapter 4, David Sindres asks this provocative question, which provides the common thread of this book. While we do not suggest a conclusive answer, our decision to edit this book reflects our view of the issue as worthy of a serious debate.

The readers should be mindful from the outset that this is not a book on the technology of the blockchain or its general relation with the law. Instead, it is an attempt to address the challenges this new technology raises from a conflict-of-laws perspective and suggest possible lines of thought. There are other books that give a more detailed introduction in the Distributed Ledger Technology and its multiple uses. The authors and the editors of this book are lawyers trained in PIL who try to identify the law governing the various assets, transactions and events of the blockchain. The literature on this subject is still very limited; to the best of our knowledge this is the first book to address conflict-of-laws issues and DLT in a comprehensive way.

2 The Distribution of Information and Assets All over the Planet

PIL seeks to administer the diversity that results from the division of the world into different states with different legal systems. It does so by submitting a particular set of facts to the law of a nation-state. Typically, this is the state with which it has its closest or most significant connection, or where it has its "seat".[2]

This principle of proximity[3] does not work well in a blockchain environment, *i.e.* where people or entities communicate and transact, peer-to-peer, on the internet, without relying on central control bodies or intermediaries. As Amy Held demonstrates at Chapter 8, the question of the "seat", or "situs", of the blockchain or the assets recorded on it poses insoluble problems. The nature of a truly global register implies omnipresence in different countries, to which the blockchain is either completely unconnected or equally strongly connected. Finding the law applicable to the blockchain thus seems like trying to nail jelly to a wall.

Of course, certain connections to the real world could be used. Chief among them are the persons acting on the blockchain. One could, for instance, refer

2 See Friedrich Carl von Savigny, *A Treatise on the Conflict of Laws*, William Guthrie (transl.) (2nd edn, T. & T. Clark 1880, reprinted by Rothman 1972), § 346 and § 360.

3 See Paul Lagarde, *Le principe de proximité dans le droit international privé contemporain : General course on private international law*, vol. 196 (Collected Courses of the Hague Academy of International Law, 1986).

to a person's habitual residence or domicile to identify the country in which the assets held or transferred by this person are most closely connected. Yet, as Anne-Grace Kleczewski explains at Chapter 6, this approach is made extremely difficult by the pseudonymity of the blockchain: while all the recordings and transfers on the blockchain are fully transparent to the whole world, the identity of the persons acting is often hidden behind a code that acts like a pseudonym, for instance, the public key in the case of the Bitcoin network. Pseudonymity causes considerable difficulty not only for the determination of the state with the closest connection, but also for the determination of the competent court and for law enforcement.

Links to the real world also exist where a blockchain asset represents an asset in the real world, such as a commodity, money or a piece of real estate. In this case, one may think of applying different conflicts rules for both, digital and physical assets. Emeric Prévost discusses this problem in detail at Chapter 10.

A complex variant of the same phenomenon are stablecoins, which represent a portfolio of real-world assets or reproduce an index or benchmark. Stablecoins have been in the limelight of regulators, but what is the private law applicable to them? Matthias Lehmann and Hannes Meyle explore this issue at Chapter 13.

3 The Lack of Choices regarding the Applicable Law and the Competent Forum

One PIL technique consists in leaving the choice of the applicable law to the parties, which is justified by the principle of "party autonomy".[4] This is especially helpful in hard cases, *i.e.* where it would otherwise be difficult or unequal to identify a strong connecting factor to a particular legal system. Moreover, the choice of law by the parties would also seem to better reflect the liberal philosophy and decentralised operation of blockchain technology, a technique that seems difficult to frame by the application of rigid connecting factors. Party autonomy, therefore, seems to be ideal to determine the law applicable to blockchain assets and transfers. The choice of the governing law could for instance be coded into the source code of the software and be imposed on

4 See Horatia Muir Watt, "Party autonomy," in Jürgen Basedow et al. (eds), *Encyclopedia of Private International Law* (Cheltenham, UK: Edward Elgar Publishing, 2017), 1337–1341; Symeon C. Symeonides, "Party Autonomy in Contract Conflicts," in Symeon C. Symeonides, *Codifying Choice of Law Around the World: An international Comparative Analysis* (New York: OUP, 2014), 109–170; Bernard Audit and Louis d'Avout, *Droit International Privé* (Paris: LGDJ, 2018), para. 238 *et seq.*, 215 *et seq.*

anyone connecting to the network. The same method could be used for the selection of the competent courts (see *infra* sub 4).

However, as Burcu Yüksel Ripley & Florian Heindler remark at Chapter 9, this approach has its limitations. Moreover, it is of little practical relevance because blockchain coders have a strong aversion to state law and courts, dating back to the first blockchain network, Bitcoin, which has apparently been developed to counter the dominant influence of states on the financial system.[5] A corollary of the distrust in the state is the distrust in its law and its institutions. Enthusiasts of the technology believe that law – and lawyers – are unnecessary because the technology itself would solve all problems likely to occur on the network. This position is summarised in the slogan "code is law" or in the belief in the existence of a *lex cryptographica* that is independent of the state; both ideas are discussed, *inter alia*, by David Sindres at Chapter 4.

Whether justified or not, the distrust of the state's legal system makes it highly improbable that coders will select an applicable state law to govern their innovations or a competent state court to settle disputes arising from them. It is therefore hardly surprising that choices of applicable law or competent courts are extremely rare in the crypto-environment and do not exist apart from some very exceptional cases, like the Corda blockchain that is developed by a consortium of traditional banks.[6] One could nurture the hope that this may be changing in the future when the coders become more "enlightened" and aware of the legal problems surrounding the blockchain, but for the moment, this is not the case. Party autonomy may be a panacea for the blockchain's PIL illness, but the patient is stubbornly refusing to take the prescribed medicine. However, the development in the future of specific choice of law rules for blockchain assets and transactions based on party autonomy, whether at the

5 In the first block of Bitcoin, the so-called genesis block, a current newspaper headline was coded: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks." This is often seen as a sly hint to the power of states to manipulate the traditional financial system. See e.g., Eric D Chason, "How Bitcoin Functions as Property Law," (2018) 49 Seton Hall Law Review 129, 132. More generally, the sociological environment from which the blockchain emerged was very critical of the state; see, on cypherpunks and crypto anarchists, e.g., Primavera De Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Cambridge, Massachusetts: Harvard University Press, 2018); see also Timothy C. May, "The Crypto Anarchist Manifesto," (*MIT*) < https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html > accessed 18 November 2022; and Eric Hugues, "A Cypherpunk's Manifesto," (*Activism*, 9 March 1993) <https://www.activism.net/cypherpunk/manifesto.html>.

6 On conflicts-of-law issues of Corda, see International Swap and Derivatives Association (ISDA) et al., "Private International Law Aspects of Smart Derivatives Contracts Utilizing Distributed Ledger Technology," (*ISDA*) <https://www.isda.org/a/4RJTE/Private-International-Law-Aspects-of-Smart-Derivatives-Contracts-Utilizing-DLT.pdf> accessed 18 November 2022.

national or international levels, might also raise more awareness regarding the advantages of a choice of law in terms of legal certainty.

4 The Characterisation Problem

Other questions arise besides the localisation issue. PIL operates on the basis of broad categories of legal relations and issues, such as contract, tort or property. Before any conflicts rule can be applied or drafted, one must therefore know the proper legal category to apply. In PIL, this problem is known as "characterisation".

The task is made difficult by the staggering variety of blockchain assets, which increases every day. There is a multitude of different types of information that are recorded on the blockchain, including coins, tokens, or smart contracts. The first step to achieve legal certainty would be a taxonomy. Some national lawmakers (*e.g.* in Switzerland) are embarking on this exercise. However, as Felix Krysa explains at Chapter 7, this is not an easy task.

Characterisation problems with regard to the blockchain had first surfaced in regulatory law. There may be cross-influences and bridges between the regulatory and the PIL world. Francesca C. Villata explores this point at Chapter 11 with regard to cryptocurrencies.

From a PIL perspective, any characterisation also has to consider the legal question that is treated. Especially difficult in this regard is the question of ownership: to whom do the blockchain assets belong? This issue can provisionally be addressed from a property law perspective without making a final determination on the proper legal characterisation. However, this approach raises other questions. PIL for property law questions traditionally distinguishes between moveables, money, and securities, and submits each to a different rule. None of these categories seems to fit virtual phenomena; trying to shoehorn them in any of these categories is elusive.

We may, therefore, need a new category. But how is it to be defined? Should it comprise only blockchain assets, or should it be broader and cover, for instance, all digital assets? One may rationally question whether DLT requires rules that are different from other assets that are stored electronically. This is the question that Christiane Wendehorst addresses at Chapter 5.

Designing a special conflicts rule for a particular type of asset is not a trivial issue but may encounter fundamental objections. As Bruno Mathis explains at Chapter 3, the principle of technological neutrality poses a particular obstacle in this regard. It may require abstraction from a currently dominant technological solution, as well as the formulation of rules that are open for future development.

The problem of characterisation is not limited to property issues; it also permeates other fields of law. Tobias Lutzi explores at Chapter 14 whether the existing conflicts rules can be applied to torts on the blockchain. Giovanni Maria Nori and Matteo Girolametti discuss issues surrounding insolvency law at Chapter 15. While these are classic conflicts fields, the blockchain forces us to see them in a new light.

The transposition of existing conflicts rules to operations on the blockchain is particularly difficult. Operations function very differently in the virtual world. The example of negotiable instruments recorded digitally and the law that applies to them is analysed by Koji Takahashi at Chapter 18. Derivatives on cryptocurrencies are another problem, which is tackled by Gregory Chartier at Chapter 19. Secured transactions on the blockchain are equally challenging; Matthias Haentjens and Matthias Lehmann make proposals for the identification of the applicable law at Chapter 16.

Sometimes the deviations between traditional operations and the crypto world are so big that one must question the application of received categories altogether. Smart contracts are an entirely new type of operation that hardly compares to the traditional contracts entered into outside the blockchain; Mehdi El Harrak analyses PIL issues they raise at Chapter 17. DAOs superficially resemble real-world co-operations but function automatically; characterisation problems surrounding them are discussed by Florence Guillaume and Sven Riva at Chapter 20.

Central Bank Digital Currencies (CBDCs), which have already been issued by some and are planned by many more states, resemble classic money. The fact that they are supported by a state seems to make the categorisation as 'money' easier than for private cryptocurrencies. Yet, they pose their own PIL problems, as Caroline Kleiner explains at Chapter 12.

5 Finding Appropriate Connecting Factors

In traditional PIL, characterisation is only a first step to identify the relevant connecting factors. In this regard, the blockchain also raises specific issues.

Thus, if we assume that crypto assets should be characterised as "property", the traditional *situs* rule cannot be extended to them, except if a "fictional" or "elective" situs can be determined (on the elective situs, see Chapter 11 by Francesca C. Villata, and with regard to the derivative market, see Chapter 19 by Gregory Chartier). Similarly, the characterisation of a DAO as a company (or legal person) can hardly imply (at least for "maverick DAOs", see Chapter 20 by Florence Guillaume and Sven Riva) the application of connecting factors traditionally used in this area, such as the seat or the place of incorporation.

As a consequence, new alternative connecting factors have been proposed, such as the place of domicile or establishment of the issuer of the tokens, although his/her identity or localisation are not always easy to determine (see Chapter 10 by Emeric Prevost regarding "digital twins"; see also, more broadly, Chapter 25 on Liechtenstein law by Francesco A. Schurr and Angelika Layr), or the place of the operator that administers the system ("PROPA", place of the relevant operating authority), or the place of the holder of the master key ("PREMA"), which could work at least for permissioned systems (see Chapter 11 by Francesca C. Villata). Another approach could be to refer to the law of the regulatory forum (see Chapter 9 by Burcu Yüksel Ripley and Florian Heindler and Chapter 24 on German law by Felix M. Wilke), which however only shifts the problem (on which criteria should the state's supervisory authority be predicated?) and might stir positive conflicts (several potentially applicable laws).

At a first look, the task seems easier when it comes to determine the law governing certain blockchain *transactions*. Indeed, the applicable law can then sometimes be determined by reference to a related off-chain transaction (this is the case, for instance, for certain types of smart contracts, such as Ricardian contracts; see Chapter 17 by Mehdi El Harrak). Even if it is not the case, the relevant connecting factors often refer to the parties involved (typically, the habitual residence of the debtor of the characteristic performance), so that a localisation of the crypto assets is not required. However, in such scenarios, the pseudonymity (or anonymity) of the parties raises additional questions.

6 Dispute Resolution

The determination of the applicable law is certainly important but cannot be envisaged in isolation from the available mechanisms for the resolution of disputes.

The identification of the court with competent jurisdiction raises similar problems regarding the determination of the applicable law. Indeed, several traditional jurisdictional criteria are not adapted to disputes related to crypto assets or to blockchain transactions, to the point that universal jurisdiction is sometimes presented as an alternative: see Chapter 20 by Florence Guillaume and Sven Riva. As these authors suggest, the traditional PIL rules on jurisdiction "usually lead to a dead-end" for disputes arising out of blockchain transactions: this is due to the pseudonymity preventing the localisation of the parties (*e.g.* DAO members or third contracting parties), the exclusive execution of smart contracts on the blockchain, and the lack of connection to state jurisdictions (*e.g.* maverick DAOs).

As we mentioned previously (see *supra* 3), party autonomy, whether in the form of choice of court or of an arbitration agreement, could be a way out.

However, for the reasons stated above (belief in the merits of technology and distrust of the states' legal systems), parties to blockchain transactions more commonly prefer to turn to blockchain dispute resolution (BDR) mechanisms. These use a combination of blockchain tokens and AI to render "on-chain" decisions that often rest on technological criteria and/or economic analysis (*e.g.* the "game theory") rather than the usual legal reasoning. Traditional PIL analysis as well as substantive law as such are deprived of all relevance in this context. Since decisions rendered in this way do not always fit within the traditional categories of "state court judgments" and "arbitral awards", classic instruments in the area of recognition and enforcement, such as the Brussels I^{bis} Regulation[7] or the New York Convention,[8] prove often to be of no use: this is the problem discussed by Pietro Ortolani in Chapter 21. By contrast, BDR decisions are often enforced "on-chain", by using technology-specific mechanisms, such as blockchain wallet escrow settings or smart-contracts. Florence Guillaume and Sven Riva at Chapter 20 discuss them in relation to DAOs.

7 The Increasing Fragmentation of Conflicts Rules with Regard to the Blockchain

Some states have reacted to the new challenges by adopting special rules for blockchain assets; a few of them have even included PIL rules in their regard. These legislative approaches are illustrated by specific country reports: for Germany by Felix M. Wilke (Chapter 24), for Japan by Tetsuo Morishita (Chapter 26), for Liechtenstein by Francesco A. Schurr and Angelika Layr (Chapter 25), for Switzerland by Pascal Favrod-Coune and Kévin Belet (Chapter 22), and for the United States by Frank Emmert (Chapter 23).

Most other countries of the world have not even started to grapple with the problem of blockchain, let alone PIL and the blockchain.We have decided to devote specific chapters only to those countries that had adopted specific legislation on the blockchain, including specific provisions on PIL aspects. We have tried our best to update and expand the list of countries during the preparation of the book. In some countries, such as Singapore or the UK, courts have been

7 Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast), [2012] OJ L351/1, 1–32.

8 United Nations Convention on the Recognition and Enforcement of Foreign Arbitral Awards of 10 June 1958.

confronted with PIL issues and have developed specific approaches. We have abstained from devoting specific chapters to those countries and preferred to leave the analyses of this case law to the authors of individual chapters.

The categories and connecting factors used in existing legislation are dazzling and the resulting picture is one of fragmentation and divergence. This calls for legal harmonisation. The prospects for the introduction of uniform conflict-of-laws rules in the blockchain area are debated in the first chapter by Gérardine Goh Escolar.

8 Outlook

The myriad of problems concerning the blockchain and PIL are highly complex. One must not be under any illusion: there is no holy grail to be found or magic stone that can be touched to solve them. Instead, one needs to engage in extensive analysis and deep reflection, as authors of contributions to this volume have done. The contributions do not offer any simple or final solutions. But they do provide a rich mine of information and ideas, which is the basis for an informed discussion.

It would be daring to predict how this discussion will end. Based on the various contributions, the discussion is unlikely to result in a single conflict-of-laws rule regarding all blockchains and digital assets. Instead, a multilevel approach is needed, which distinguishes between different legal issues and various types of networks. Depending on the question to be answered, it may also be necessary to treat different digital assets and certain transactions differently.

We are not in a position to formulate such rules here, but we can formulate certain conditions that they should fulfil. In particular, they should mirror the needs and the legitimate expectations of the parties involved, and reflect the particularities of the blockchain. But they should not focus merely on the blockchain; instead, they should be sufficiently open to accommodate further technological developments.

Most of all, it is to be wished that the conflict-of-laws rules be as uniform as possible around the world. This is the only response appropriate to a technology whose nature is global. If states were to differ in their determination of the law applicable to the blockchain, and the transactions and assets recorded on it, tremendous legal uncertainty and protracted legal disputes would certainly be the result. There is a risk that the benefits of the innovative DLT cannot be fully enjoyed where the conflict-of-laws rules vary. The experience of PIL demonstrates that such divergences can best be overcome by a transnational approach: let the debates begin!

CHAPTER 1

The Role and Prospects of Private International Law Harmonisation in the Area of DLT

Gérardine Goh Escolar

1 Introduction[1]

Distributed ledger technology (DLT) is increasingly deployed as a solution for daily operations. DLT finds applications in sectors and use cases such as financial technology (FinTech), smart contracts, derivatives, proof of ownership, asset traceability and digital currency. Its massive potential for a wide range of applications has taken DLT from the rarefied atmosphere reserved only to the most technology-savvy elite to the pockets and desks of many around the world in the form of mechanisms that increase systems robustness and operational efficiency.

DLT and its applications find uses in many commercial sectors and has been the subject of significant investment as a result. However, many Private International Law (PIL) issues remain. Questions relating to the determination of the applicable law, jurisdiction, choice of forum, and recognition and enforcement remain unresolved. The complexity of answers to these questions is further compounded due to the global reach of DLT applications, which do not recognise traditional national borders and thus require novel approaches to traditional concepts in PIL.

At present, for example, there is no clear PIL solution either in relation to the applicable law to digital assets and corresponding transfers, or in relation to the possibility of incorporating party autonomy and choice of law in DLT protocols. Additionally, there is also no clarity as to which State has the jurisdiction to resolve disputes that may arise, with the very rare

1 The author thanks Harry Cheng for his invaluable support in the preparation of this chapter, Christophe Bernasconi and Ning Zhao for their input, as well as Jana Araji, Nadia Bouquet, Ilia Lassin, Jaime Vazquez Garcia, Rachel van der Veen and Deannie Yap for their research assistance. Opinions in this chapter do not engage the organisations with which the author is affiliated. Any errors in this chapter remain entirely those of the author.

© GÉRARDINE GOH ESCOLAR, 2023 | DOI:10.1163/9789004514850_003
This is an open access chapter distributed under the terms of the CC BY-NC-ND 4.0 license.

exception in which the dispute concerns transactions in which all nodes are located in one State (*i.e.*, one-jurisdiction, permissioned systems). Moreover, the applicability and enforceability of choice of court agreements involving digital assets still hang in the balance.

This chapter will consider the PIL challenges arising from DLT applications, including the considerations that arise in specific DLT use cases. It will discuss the role of PIL harmonisation in DLT, and the ongoing work at the Hague Conference on Private International Law (HCCH), the United Nations Commission on International Trade Law (UNCITRAL) and the International Institute for the Unification of Private Law (UNIDROIT) to harmonise PIL rules that relate to DLT applications. It will then touch on the prospects for such harmonisation, before looking to the future of PIL in the DLT space. To set the stage for this discussion, this chapter first briefly discusses the context of DLT applications and the characteristics of DLT that trigger these PIL challenges.

2 Context

2.1 *What is DLT?*

DLT has been defined as:

> ...the practice that uses nodes...to record, share and synchronize transactions in their respective electronic ledgers (instead of keeping data centralized as in a traditional ledger). The participant at each node of the network can access the recordings shared across that network and can own an identical copy of it. Any changes or additions made to the ledger are reflected and copied to all participants in a matter of seconds or minutes.[2]

DLT is the protocol on which blockchain is based.[3] DLT consists of a register ("ledger") distributed across an online network without a central control

2 United Nations Conference on Trade and Development (UNCTAD), "Harnessing Blockchain for Sustainable Development: Prospects and Challenges" (*UNCTAD*, 25 June 2021), 50 <https://unctad.org/system/files/official-document/dtlstict2021d3_en.pdf>.

3 See also Hague Conference on Private International Law (HCCH), "Developments with respect to PIL implications of the Digital Economy" (*HCCH*, March 2022), para. 13 <https://assets.hcch.net/docs/b06c28c5-d183-4d81-a663-f7bdb8f32dac.pdf>.

point.[4] A network of computers cryptographically identifies users and validates interactions among users before recording the interactions across the network of identifying and validating computers.[5] Individuals or entities interacting through the system are identified with a pair of cryptographic keys: a public key that acts like an address, and a private key that acts like a password. Any computer connected to the network is referred to as a node. Each of these nodes operates a full copy of validated transactions of the blockchain ledger.[6] Packages of data that carry the recorded data on the network are called "blocks". Each block is definitively linked to the next block using a cryptographic signature, creating a "chain". This allows "blockchains" to act as a ledger that can be accessed and shared with the appropriate permissions.[7]

2.2 *Characteristics of DLT That Impact PIL Considerations*

In considering the characteristics of DLT that may impact PIL considerations, a point of note is that there are many ways of designing, implementing and employing DLT. The characteristics of each DLT system impact the use cases best suited to it and raise different PIL issues.[8] It is particularly important, however, that any initiative aimed at harmonising PIL should focus on the applications of DLT, and should, while addressing the particularities of DLT-based systems and applications, be as technology-neutral and -agnostic as possible.[9]

---

4 UNCTAD (n 2), 2.

5 See *e.g.*, Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (*Bitcoin*) <https://bitcoin.org/bitcoin.pdf> accessed 15 December 2022; Vitalik Buterin, "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform" (*Ethereum*, 2014) <https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Buterin_2014.pdf> accessed 15 December 2022 (the Ethereum Whitepaper, elaborating on the functioning of blockchains as well as smart contracts).

6 UNCTAD (n 2), 51.

7 *Id.*

8 On the use case analysis of DLT by asset class and product line, see the World Economic Forum (WEF), "Digital Assets, Distributed Ledger Technology and the Future of Capital Markets: Insight Report" (*WEF*, May 2021), 32–86 <https://www3.weforum.org/docs/WEF_Digital_Assets_Distributed_Ledger_Technology_2021.pdf> accessed 15 December 2022.

9 For a discussion on the principle of technological neutrality, the pillars on which this principle is built, and the legislative issues that come up with respect to the definition of legal objects, the design of technology rules and their impact on PIL, see Chapter 3 of this book by Bruno Mathis, "Should Crypto-Asset Regulation be Technology-neutral?". For arguments that a possible international instrument relating to PIL should be technologically neutral and be able to accommodate interplay between bodies of law such as

The first such characteristic is the *decentralised* nature of DLT, which operates across traditional jurisdictional borders, has a great impact on considerations of PIL. The decentralised record of transfers of digital assets across multiple internet servers ("nodes") in a DLT mechanism means that transfers are in many cases *disintermediated*. Moreover, transactions and relationships that are created via DLT are multi-party and request multi-signatures for their conclusion, thereby allowing the network to include self-enforcing adjudication within its activities.[10]

The second is that actions from outside of the DLT network cannot prevent transactions from being made within the DLT network, which are partly *automated*. A transaction, once triggered, sets in motion a series of concatenated, previously coded, virtual actions. For this reason, there has been support for the existence of a "rule of code" in DLT environments, because some of these actions are independent of direct human intervention.[11]

Third, transactions in DLT networks are *immutable*. The immutability of DLT transactions provides security against tampering, but in the same vein, they have also been classified by some actors as "disruptive" of existing legal frameworks. Following on the same line of reasoning, some have taken the view that traditional concepts of contract law, including excuses for non-performance such as hardship or *force majeure* cannot, and indeed do not, apply.[12]

Fourth, the pseudonymity of users and the decentralised nature of the ledger make it difficult to determine the *situs* of a transaction.[13] This difficulty in determining the *situs* has led to differing views as to whether analogies can

---

family, succession, intellectual property, insolvency and so on, see Chapter 9 of this book by Burcu Yüksel Ripley and Florian Heindler, "The Law Applicable to Crypto Assets: What Policy Choices are Ahead of Us?".

10 See HCCH, "Developments with respect to PIL implications of the digital economy, including DLT" (*HCCH*, March 2021), paras. 11–14 <https://assets.hcch.net/docs/8bdc7071-c324-4660-96bc-86efba6214f2.pdf> accessed 15 December 2022.

11 See, for example, the Financial Markets Law Committee (FMLC), "Distributed Ledger Technology and Governing Law: Issues of Legal Uncertainty" (*FMLC*, March 2018), 21 <http://fmlc.org/wp-content/uploads/2018/05/dlt_paper.pdf> accessed 15 December 2022.

12 See (n 10), para. 8.

13 Matthias Lehmann (2019) "Who Owns Bitcoin? Private (International) Law Facing the Blockchain," (2019) European Banking Institute Working Paper Series no. 42, 2. For a discourse on the pseudonymity related to DLT appications and its impact on PIL considerations, see Chapter 6 of this book by Anne-Grace Kleczewski, "The Good, the Bad and the Ugly: The Private International Law, the Crypto Transactions, and the Pseudonyms".

be drawn from legal frameworks in existing regimes, such as intellectual property[14] or goodwill in a business,[15] or whether this difficulty justifies taking an entirely novel approach.[16] The debate has been compounded by the fact that the perimeters of many domestic legal institutions appear to be insufficient to address the difficulties raised by the cross-border nature of DLT applications. There has also been discussions as to whether the larger-scale applications serviced by Blockchain 3.0 illustrate that "[n]o one solution can fit all DLT systems".[17]

These four characteristics of DLT-based assets, agreements and operations impact on traditional considerations of PIL. The next section will consider the specific PIL challenges brought on by DLT applications.

3 *PIL* Challenges Brought on by DLT Applications

Specific PIL challenges arising from DLT applications include:

> Terminology (*e.g.,* what is the definition of "digital assets" on a blockchain),
> Applicable law and choice of law (*e.g.*, what is the most appropriate connecting factor defining the law applicable to a transaction via blockchain),
> Jurisdiction and choice of court (*e.g.*, how to determine the competent court to resolve a dispute in relation to a crypto asset), and
> Recognition and enforcement (*e.g.*, how to enforce a foreign judicial decision in relation to a service regulated by a smart contract).

This section will look at each of these challenges in turn.

---

14 Gerald Spindler, "Fintech, digitalization, and the law applicable to proprietary effects of transactions in securities (tokens): a European perspective" (2019) 24 Uniform Law Review 724, 736–737.10 See HCCH, "Developments with respect to PIL implications of the digital economy, including DLT" (*HCCH*, March 2021), paras. 11–14 <https://assets.hcch.net/docs/8bdc7071-c324-4660-96bc-86efba6214f2.pdf> accessed 15 December 2022.

15 Andrew Dickinson, "Cryptocurrencies and the Conflict of Laws," in David Fox and Sarah Green (eds), *Cryptocurrencies in Public and Private Law* (OUP 2019), paras 5.107–5.121.

16 Michael Ng, "Choice of law for property issues regarding Bitcoin under English law," (2019) 15 Journal of Private International Law 315, 316.

17 See (n 11).

3.1 *Terminology*

The terminology used in discussing the different technologies, systems and applications in the digital economy, including those based on DLT, is a topic that is increasingly discussed in different fora. The lack of uniformity and harmonisation in these discussions comprise one of the main challenges of DLT, a technology that is both application-agile and evolving.

There have been concerted efforts to harmonise terminology being used, including initiatives by the Blockchain Terminology Project of InterPARES Trust.[18] UNCITRAL and UNIDROIT are also jointly and separately hosting Working and Experts' Groups that are working on the development of legal taxonomies.[19] The HCCH contributes to the work of its sister organisations UNCITRAL and UNIDROIT as an observer to these Working and Experts' Groups.

3.2 *Applicable Law and Choice of Law*

DLT-based applications give rise to various challenges in relation to the applicable law. In this regard, specific questions arise on the issues of characterisation, connecting factors, and the scope and limits on party autonomy.

3.2.1 Characterisation

One challenge to the determination of the applicable law that arises relates to the legal nature of the asset. Some jurisdictions consider that some assets traded in decentralised systems are tangible assets while others are not ("off-platform tokens" vs "on-platform tokens"). There is as yet no harmonised view or approach on this issue.[20]

---

18 See InterPARES Trust Terminology Database, available at: http://interparestrust.org/terminology .

19 United Nations Commission on International Trade Law, "Legal issues related to the digital economy" (*UN*, 8 May 2020), 4 <https://documents-dds-ny.un.org/doc/UNDOC/GEN/V20/024/68/PDF/V2002468.pdf?OpenElement>. The UNIDROIT Working Group on Digital Assets and Private Law is working on guidance that also deals with the matter of terminology, see for an overview of its work: International Institute for the Unification of Private Law (UNIDROIT), "Digital Assets and Private Law" (*UNIDROIT*) <https://www.unidroit.org/work-in-progress/digital-assets-and-private-law/#1622753957479-e442fd67-036d> accessed 15 December 2022.

20 For a discussion of a taxonomy for crypto-of crypto assets and therefore the PIL rules that apply to those assets, see Chapter 7 of this book by Felix Krysa, "Taxonomy and Characterisation of Crypto Assets".

3.2.2 Connecting Factors

The traditional connecting factors that relate to geographical locations ("*situs*") may not be of relevance to the functioning of a DLT network.[21] There is broad recognition that the concept of *situs* poses challenges for a PIL framework concerning digital assets, because it is technically and legally difficult to identify the location where assets on the ledger are located.[22] In addition, the pseudonymity of users, the immaterial nature of digital assets, and the uncertainty of the location of network nodes increase the difficulty of identifying useful connecting factors.[23]

In this regard, the difference between permissioned and permissionless systems in the DLT platforms may be crucial in determining what the applicable law is. Individuals on permissioned ledgers must be authorised before they can gain access to the system, thus becoming identifiable. On the other hand, users are not required to obtain permission to participate in permissionless systems, which are usually based on open-source software.

To connect DLT systems to a geographical location, novel formulations have developed, for example, the "Place of the Relevant Operating Authority / Administrator" (PROPA). For systems that function with a master key, there is also the "Primary Residence of the Encryption Private Master Keyholder" (PREMA). Rather than focus on the location of the asset or the place where the transaction was made, the location of the participant (*e.g.*, the consumer) or the relevant operating authority is made the focus instead. Table 1.1: An Overview of Connecting Factors shows an overview of connecting factors that have appeared in the PIL discourse relating to DLT systems and applications.

---

21 For a detailed discussion of the basics of DLT and the connecting factors relevant to the most characteristic use cases of DLT, see Chapter 2 of this book by Tetsuo Morishita, "Technical Description of DLT with a Focus on Possible Connecting Factors".

22 HCCH Conference on Commercial, Digital and Financial Law Across Borders (CODIFI Conference), all contributions available on the HCCH YouTube channel, available online at <https://www.youtube.com/playlist?list=PLL3fQvUXrbUE0D2Oevr8VoAYUXIQ1AD-_> accessed 15 December 2022; CODIFI Conference, Amy Held, "Digital Economy / PIL & DLT: What Challenges Lie Ahead?," 15 September 2022; CODIFI Conference, Sarah Green, "Digital Economy / How is Applicable Law Best Determined – By Asset, System or Transaction?," 13 September 2022. For an examination of the private international law rules relating to *lex situs* and *forum situs* regarding decentralised ledgers and crypto-assets, see Chapter 8 of this book by Amy Held, "Crypto Assets and Decentralised Ledgers: Does *Situs* Actually Matter?".

23 CODIFI Conference, Andrea Bonomi, "Opening of the Digital Economy 'Frameworks' Track," 12 September 2022; CODIFI Conference, Teresa Rodriguez de Las Heras Ballell, "Digital Economy / Expanded Applications of DLT: Supply Chain," 14 September 2022.

TABLE 1.1 Overview of connecting factors[24]

Rule and Description	Advantages	Limitations
LEX SITUS[25]	TANGIBLE PROPERTY	DISTRIBUTED AND DECENTRALISED
Traditional PIL property rule. With the historical focus on tangible goods, *lex situs* dictates that rights or entitlement should be governed by law of the place in which the property or claim to property is situated.	For DLT arrangements exchanging 'exogenous tokens'[26] that represent tangible property (especially immovable property), courts will most likely apply the *lex situs* of the underlying asset. For exogenous tokens, changes to existing conflict rules may not be necessary, as the only difference lies in the technology underpinning the transaction. Here, traditional conflict rules may be more appropriate.	*Lex situs* rule does not translate well when applied to a DLT system. Situs of an asset constituted on a DLT ledger is not obvious for two reasons. First, because the ledger is distributed. A network can span several jurisdictions and have no central authority or validation point (especially in permissionless systems). Second, location may be hard to determine for cross-border transfers of intangible assets. Application of geographically-dependent connecting factors are problematic in DLT context.

(*Continued*)

24 This table was originally annexed to HCCH (n 10), Annex I.

25 FMLC (n 11), 10.

26 Distinction between "endogenous tokens" (*i.e.*, native cryptocurrencies) and "exogenous tokens." Endogenous tokens do not refer to anything existing outside the blockchain. Exogenous tokens are those which have a necessary connection with assets existing outside the blockchain. UNIDROIT, "Joint UNCITRAL/UNIDROIT Workshop" (*UN*, 2019), 2 <https://www.unidroit.org/english/news/2019/190506-unidroit-uncitral-workshop/conclusions-e.pdf> accessed 15 December 2022.

TABLE 1.1 Overview of connecting factors (*Continued*)

Rule and Description	Advantages	Limitations
ELECTIVE SITUS[27] Proprietary effects of DLT transactions governed by the chosen law of the DLT network participants.	***SIMPLICITY AND CERTAINTY, ESPECIALLY FOR REGULATION*** Proprietary effects of all transactions on the system are subject to the same governing law. Applicable law of the transaction is transparent to participants and regulation.	***THRESHOLD ISSUES, REGULATORY RISKS*** Two threshold issues. First, party autonomy is not universally accepted as a choice-of-law principle for proprietary issues. Second, it may be difficult to apply in permissionless systems.[28] More significant issue will likely be the perceived regulatory risks. For instance, participants may choose a legal system unrelated to the assets and is subject to significant undue influence. This could potentially facilitate the mass transfer of assets by means of legal adoption in the jurisdiction identified by the connecting factor.

27 FMLC (n 11), 15.

28 For permissioned systems, acceptance of a particular governing law could be included in terms for accession to the system (*e.g.*, clearing houses). Norton Rose Fulbright, "Legal analysis of the governed blockchain" (*Norton Rose Fulbright*, June 2018), 1 <https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/imported/emea_4957_online-publication-and-pdf__legal-analysis-of-the-governed-blockchain_v4.pdf?la=en&revision=c15aa8eb-48d5-4d06-8851-8226bdb1145f> accessed 15 December 2022 describes these terms of access as the "Constitution" of a permissioned "governed" blockchain – without which the blockchain would be permissionless.

TABLE 1.1 Overview of connecting factors (*Continued*)

Rule and Description	Advantages	Limitations
MODIFIED ELECTIVE SITUS[29] A variant of the 'elective situs' rule. The participants' choice of *situs* could be restricted by regulation or technology. For example, election could be limited to a choice of law approved by regulators, or restricted in respect of a choice of law lacking any connection to the DLT enterprise.	***ADDRESSES PUBLIC POLICY CONCERNS*** Regulators may consider this necessary if uninhibited choice of parties is perceived as being used for avoidance purposes, or that such free choice would contradict public policy.[30]	Approval from more than one regulator. May be difficult to implement rule that requires approval from more than one regulator – especially where the competent authority for a distributed system is not obvious.
DEEMED ELECTION[31] Another variant of the 'elective situs' rule. Deemed election is determined by relevant regulatory or competent authority, where applicable.	***SIMPLICITY AND TRANSPARENCY*** Proprietary effects of all transactions are subject to the same governing law. Transparency to third parties – assuming that the deemed election would be public knowledge.	***IDENTIFYING THE COMPETENT AUTHORITY*** May be self-defeating. A further rule on determining the relevant national competent authority is needed.

(*Continued*)

29 FMLC (n 11), 16.

30 Although not mentioned in the FMLC Report, Article 4 of the HCCH 2006 Securities Convention, which conditions the validity of the choice of law agreement to the relevant intermediary having an office in that State, meeting certain minimum criteria, provides an example of this kind of restriction on the elective situs. Further, Article 11 of the HCCH 2015 Principles on Choice of Law in International Contracts provides limitations resulting from overriding mandatory rules and public policy (*ordre public*). The FMLC Report mentioned Rome I Regulation as an example, as it restricts party autonomy in choice of law by preserving certain protective rules, rather than by limiting the possible options.

31 FMLC (n 11), 17.

TABLE 1.1 Overview of connecting factors (*Continued*)

Rule and Description	Advantages	Limitations
CHOSEN LAW OF THE TRANSACTION/ TRANSFER/ ASSIGNMENT[32] In the context of one or more transfers of an asset, proprietary effects of the transaction are determined by the applicable law of the assignment.	***PARTY AUTONOMY, SIMPLICITY*** Applying the law of assignment allows parties to choose the law that will govern proprietary effects of the transaction. Simplicity and coherence regarding the choice of law rule on contractual effects.	***COMPETING ENTITLEMENTS, PRACTICAL DIFFICULTIES, FRAGMENTATION*** No certain answer in case of competing entitlements where successive transfers take place under different governing laws. Requires participants in DLT system to coordinate and agree on governing law. Practical difficulty and inefficiency of this requirement undermines the speed and efficiency of using DLT. Fragmentation within a DLT system, where recorded transactions are subject to multiple different laws.

32 *Id.*

TABLE 1.1 Overview of connecting factors (*Continued*)

Rule and Description	Advantages	Limitations
PROPA[33]	***CERTAINTY***	***RELOCATION OF R(O)A, IDENTIFYING THE R(O)A, PERMISSIONLESS SYSTEMS.*** *See 'PREMA' below for 'costs.'*
Place of the Relevant Operating Authority/ Administrator. This rule presupposes that the DLT system is both (i) permissioned and (ii) centralised (under the control of a central operating authority or administrator). For such a system, the governing law would either be (i) the location of the R(O)A[34] or (ii) the R(O)A is responsible for determining the governing law.		The PROPA rule is problematic where the R(O)A is required to move jurisdictions (e.g. Brexit). May not always be clear who the R(O)A is. Whether an authority should be the R(O)A may change depending on the role of the administrators.[35] Furthermore, additional rules are required to choose between two R(O)A candidates have equivalent powers and are located in different jurisdictions. Most importantly, PROPA would not be applicable in systems without R(O)As, specifically – permissionless and 'trustless' DLT systems.

(*Continued*)

33 *Id*. at 18.

34 Relevant Operating Authority/Administrator.

35 For instance, an administrator's role may be limited to verifying participants' identity or providing technical access to the ledger. It is uncertain as to what functions and purposes an administrator must serve in order to qualify as an R(O)A.

TABLE 1.1 Overview of connecting factors (*Continued*)

Rule and Description	Advantages	Limitations
PREMA[36]	***CERTAINTY***	***TERTIARY 'WARRANT' KEY, COSTS***
Primary Residence of the Encryption Private Master keyholder. Similar to PROPA, but this approach looks to the location of the private master key[37] for the DLT system (for systems that have such a key). Presumptively, this location would be the primary residence, centre of main interests or (possibly) domicile of the master key-holder.		A significant disadvantage of PREMA is the increasing prevalence of tertiary 'warrant' keys. These keys allow DLT enterprises to decrypt data if they are served with a court order. For both PROPA and PREMA, legal opinion must be sought in locating the R(O)A/ master key holder, thereby increasing costs for market participants.
LOCATION OF ISSUER MASTER ACCOUNT[38]	***ENFORCING CLAIMS***	***ACTION AGAINST SYSTEM ADMINISTRATOR***
For securities issues, this looks to the place of the issuer master account where there is no intermediary and investors hold securities directly from the issuing company.	In addition to other advantages (simplicity, certainty), this rule aligns choice of law with the legal system under which claims must ultimately be enforced against the issuer.	By contrast, a disadvantage of this rule is the lack of alignment between choice of law and the legal system under which regulatory or legal action against the system administrator can be most effectively taken.

36 FMLC (n 11), 19.

37 This would be the key by which the R(O)A or relevant authority controls the ability to transfer digital assets on the ledger.

38 FMLC (n 11), 19.

TABLE 1.1 Overview of connecting factors (*Continued*)

Rule and Description	Advantages	Limitations
LOCATION OF PARTICIPANT[39] Applies law of the place where the system participant (*i.e.*, who is transferring assets) is resident, has centre of main interest, or is domiciled.	***BULK TRANSFERS*** Appropriate for transfer of assets in bulk. Otherwise, transferees would have to conduct due diligence on each asset under its own governing law or *lex situs* respectively.	***RELEVANCE, QUESTIONS OF ENTITLEMENT, SPLITTING THE LEDGER*** Questionable relevance of this benefit (*left, 'bulk transfers'*) in a DLT environment. A significant disadvantage is that this rule gives no clear answer to questions of entitlement where there are: joint transferors, chains of assignments, or change in habitual residence by the transferor. Rule artificially splits up the distributed ledger record.

(*Continued*)

39 *Id.* at 19–20.

TABLE 1.1 Overview of connecting factors (*Continued*)

Rule and Description	Advantages	Limitations
LAW OF PRIVATE USER KEY[40]		***DETERMINING LOCATION, COSTS***
Location of private user key[41] for the DLT system. This would presumptively be the primary residence, centre of main interests or (possibly), domicile of user key-holder.		May be difficult to objectively determined domicile of user key-holder, especially because one key may be composed of several parts that are held across multiple jurisdictions. Establishing location of the relevant person will necessitate complex legal opinions and cost.
LAW OF THE ASSIGNED CLAIM[42]	***ELECTIVE SITUS, WIDER CONFLICTS REGIME***	***ONLY APPLICABLE TO EXOGENOUS INTANGIBLE ASSETS***
Proprietary effects of transaction would be governed by the applicable law of the assigned claim. Understood as a kind of *situs* rule for intangible assets. Here, the *situs* is deemed to be the legal system identified as the applicable law of the asset.	This approach enjoys the same advantages as with an elective *situs* rule. For the EU, it would also have the benefit of aligning with the wider conflicts of law regime (Rome I).	Rule can only be implemented for intangible assets that have a separate existence from the DLT system (*i.e.,* must not be tangible assets or native 'on-platform'[43] tokens). As previously mentioned, tangible assets will likely be

40 FMLC (n 11), 20.

41 Key by which a participant in the system controls the digital asset.

42 FMLC (n 11), 20.

43 Depending on whether the distributed ledger is a blockchain, the term "on-platform" may be used interchangeably with "on-chain." The same applies for "off-platform" and "off-chain."

TABLE 1.1 Overview of connecting factors (*Continued*)

Rule and Description	Advantages	Limitations
		governed by *lex situs*. As for virtual 'on-chain' endogenous tokens, a separate rule tailored to the distributed system is required.
LEX CODICIS[44] *Also: lex digitalis, PResC*.[45] Looks to the governing law of the code that was used to create the original distributed ledger programme. Usually taken to be the Primary residence of the original Coder (PResC).	***SIMPLICITY AND CERTAINTY*** Original coder can be identified relatively easily. Rule also provides *ex ante* certainty.	***RELEVANCE OF ORIGINAL CODER*** Tenuous connection to the original coder. Where the coder is not also the system administrator, there is little reason why they should be relevant to and responsible for subsequent developments on the distributed ledger.

The challenges inherent in applying traditional connecting factors to assets on DLT platforms has also led to the creation of novel types of connecting factors that involve information technology criteria. One example is the formulation of a "*lex codicis*" or "*lex digitalis*", which considers the governing law of the code that was used to create the original distributed ledger programme. In the case where the computer code itself does not have a particular *situs*, the governing law of the code is taken to be the primary residence of the coder (or PResC).[46]

Industry players have advocated a deeper analysis of possible connecting factors, which would enhance the legal understanding of blockchain assets as

44 FMLC (n 11), 21.
45 Primary Residence of the Coder.
46 FMLC (n 11), 21.

they evolve.[47] This is preferable to a static approach that lays out how blockchain assets should be classified, as the way forward should have flexibility to adopt to new and creative blockchain assets. For example, some experts have opined that a proxy for geographic *situs* needs to be found for digital assets since they do not possess a physical location.[48] Emerging approaches to this problem have focused on examining explicit choices of law, such as Article 12 of the 2022 Uniform Commercial Code Amendments. This article provides a "waterfall" of alternatives for determining the governing law of a "controllable electronic record".[49] "The primary rules of this waterfall require for their applicability express provisions of a controllable electronic record, an attached or logically associated record, or the system in which a controllable electronic record is recorded"; as last resort, the law of the District of Columbia is applied.[50] Similarly, the draft principles of the UNIDROIT Digital Assets Working Group adopt a waterfall of four factors to discern the applicable law – the first consideration would be to apply the law that is applicable to the custodian of the crypto asset, since most crypto assets are held by an exchange or wallet.[51]

3.2.3 Party Autonomy

Another challenge to the determination of applicable law is the growing movement that seeks to differentiate between actions inside and outside of a blockchain ("on-chain" vs "off-chain"). This differentiation has impact on party autonomy because there is no guarantee that a *situs* chosen by the parties in off-chain agreements will be effectively applicable.[52]

---

47 CODIFI Conference, Tju-Liang Chua, "Interview with the General Counsel of Ethereum," 12 September 2022.

48 CODIFI Conference, Hin Liu, "Digital Economy / Digital Assets Remedies," 15 September 2022.

49 Official Comment to Article 12, available at Uniform Law Commission, "UCC, 2022 Amendments to" (*ULC*) <https://www.uniformlaws.org/viewdocument/final-act-164?CommunityKey=1457c422-ddb7-40b0-8c76-39a1991651ac&tab=librarydocuments> accessed 15 December 2022.

50 *Id.*

51 For a discourse on digital assets that are held by a (crypto-)custodian and those that are not, and an argumentation that the custodian forms the closest connecting factor in the area of secured transactions, see Chapter 16 of this book by Matthias Haentjens and Matthias Lehmann, "The Law Governing Secured Transactions in Digital Assets".

52 On the law applicable to digital representations of off-chain assets, including tentative approaches to proprietary and private international law rules relating to tokenised assets and digital twins, see Chapter 10 of this book by Emeric Prévost, "The Law Applicable to Digital Representations of Off-Chain Assets".

Some experts have proposed a party autonomy-focused approach that allows the applicable law to be chosen by the parties.[53] One example, reflecting the draft principles of the UNIDROIT Digital Assets and Private Law Working Group, is to adopt a "waterfall" of four factors to discern the applicable law.[54] Under this approach, the first consideration is to apply the law that is applicable to the custodian of the crypto asset, since most crypto assets are held by a crypto exchange or wallet.[55] Other possible options may be tied to the system on which the asset was created.[56] In the absence of explicit choice of law, another alternative approach may rely on the law of the place of characteristic performance.[57]

3.2.4 Revision and Use of Existing Frameworks to Determine the Applicable Law

There is broad consensus that, where possible, it would be preferable to use existing frameworks (for example, in existing insolvency law) rather than developing new connecting factors exclusively for an existing field's intersection with DLT.[58] Experts have also discussed the possibility of revising PIL rules applicable to negotiable instruments, particularly to ensure that the party autonomy principle could be applied and to take into account how digitalisation transforms core features of negotiable instruments, namely the place of signature and physical possession requirements.[59]

Experts have also noted that the HCCH 2015 Principles on the Choice of Law in International Commercial Contracts[60] could be relevant to DLT applications. Clarity on choice of law would be crucial in this context, as the parties'

---

53 CODIFI Conference, Emeric Prévost, "Digital Economy / Loi applicable: determination par actif, par système ou par transaction?," 13 September 2022.

54 UNIDROIT, "Master Copy of the Draft Principles and Comments" (*UNIDROIT*, December 2022) <https://www.unidroit.org/wp-content/uploads/2022/12/W.G.7-Doc.-2-Draft-Principles-and-Commentary.pdf> accessed 15 December 2022.

55 CODIFI Conference, Matthias Lehmann, "Digital Economy / How is Applicable Law Best Determined – By Asset, System or Transaction?," 13 September 2022.

56 CODIFI Conference, Louise Gullifer, "Digital Economy / Characterising Relationships Between Asset Holders and Exchanges," 13 September 2022.

57 CODIFI Conference, Kelvin Low, "Digital Economy / How is Applicable Law Best Determined – By Asset, System or Transaction?," on 13 September 2022.

58 CODIFI Conference, Florian Heindler, "Digital Economy / PIL & DLT: What Challenges Lie Ahead?," 15 September 2022.

59 CODIFI Conference, Benjamin Geva and Sagi Peari, "Securities / Negotiable Instruments," 14 September 2022.

60 HCCH, "Principles on Choice of Law in International Commercial Contracts," (*HCCH*, 19 March 2015) <https://www.hcch.net/en/instruments/conventions/full-text/?cid=135> (HCCH 2015 Principles).

choice would be an important consideration when circumstances could make it difficult to localise contracts in one State.[61] Experts considered the potential application of the HCCH 2015 Principles to issues such as smart contracts based on DLT systems and for transactions such as cross-border transfers of data, which remain largely subject to different national laws.[62]

3.3 *Jurisdiction and Choice of Court*

The allocation of jurisdiction among national courts is another PIL issue that arises in relation to digital assets based on DLT.

One example is in the case of Initial Coin Offerings (ICOs), which triggered a wave of class actions filed in the USA. The court of the Northern District of California discussed the matter of jurisdiction in relation to such digital assets in the case of *Tezos*, where it considered "the operative question" of "where does an unregistered security, purchased on the internet, and recorded "on the blockchain," actually take place?"[63] In its Order, the court considered the various aspects of the sale, noting the location of the server that hosted the website in question, the location of the individual who operated the website, and the fact that the transaction was validated by a network of global nodes clustered most densely in the United States. The court found that, "[w]hile no single one of these factors is dispositive to the analysis, together they support an inference that [the] alleged securities purchase occurred inside the United States."[64]

3.4 *Recognition and Enforcement*

Dispute resolution and remedies awarded may also pose various challenges depending on the asset and the system in question. The valuation of an asset under dispute, for example, could depend on whether it is unique or fungible, and this determination could condition whether or not an injunction may be

---

61 CODIFI Conference, Benjamin Geva and Sagi Peari, "Securities/ Negotiable Instruments," 14 September 2022.

62 CODIFI Conference, Florence Guillaume, "HCCH Principles / The HCCH Principles and the Digital World (French Session)," 15 September 2022.

63 *In re Tezos Securities Litigation*, (N.D. Cal.), Case no. 17-cv-06779-RS, Order on Defendants' Motion to Dismiss (available online at <https://storage.courtlistener.com/recap/gov.uscourts.cand.319743/gov.uscourts.cand.319743.148.0.pdf> accessed 15 December 2022). For an analysis of this decision, see Koji Takahashi, "Prescriptive Jurisdiction in Securities Regulations: Transformation from ICO (Initial Coin Offering) to the STO (Security Token Offering) and the IEO (Initial Exchange Offering)," (2020) 45 Ilkam Law Review 31, 42.

64 *In re Tezos Securities Litigation, supra* note 63, at 13–14.

granted.[65] Given that courts may issue orders compelling certain assets to be turned over, difficulties that may arise include questions of whether a turnover order against automated smart contracts can be enforced, or how to access digital assets in the case private keys have been lost. At present there is no effective and practical means of execution of virtual assets, and no harmonisation across jurisdictions as to the recognition and enforcement of these types of orders.[66]

Experts moreover agree that there is a lacuna in cross-border dispute-resolution law. Specifically, the absence of a non-institutional set of rules, such as the UNCITRAL Model Law on International Commercial Arbitration,[67] means that there is no framework that may be partially self-enforced on the blockchain and partially enforceable off-chain.[68] There may also be difficulties in deciding where to initiate recognition and enforcement proceedings of a transaction carried out, for example, in a metaverse.[69] In these cases, it has been argued that allowing the claimant to bring proceedings before the courts of their habitual residence may be a potential solution.[70]

4 Case Studies: PIL Considerations in DLT Use Cases

The continued optimism in the outlook on Web3 and the digital economy has fuelled the recent widespread decoupling of DLT use cases. This has led to the validation and adoption of concrete and sector-specific use cases, as well as

65 For an excellent discussion of the outcome of blockchain-based dispute resolution, see Chapter 21 of this book by Pietro Ortolani, "Recognition and Enforcement of the Outcome of Blockchain-Based Dispute Resolution".

66 CODIFI Conference, Andrew Hinkes, "Digital Economy / Digital Assets Remedies," 15 September 2022.

67 UNCITRAL, "UNCITRAL Model Law on International Commercial Arbitration (1985), with amendments as adopted in 2006" (*UNCITRAL*, 2008) <https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/19-09955_e_ebook.pdf> accessed 15 December 2022.

68 CODIFI Conference, Pietro Ortolani, "Digital Economy / Blockchain-Based Dispute Settlement Mechanisms (Ortolani)," 14 September 2022.

69 CODIFI Conference, Juliette Asso, "Digital Economy / Expanded Applications of DLT: Metaverses," 14 September 2022.

70 CODIFI Conference, Laura Azaria, "Digital Economy / Expanded Applications of DLT: Supply Chain," 14 September 2022.

the unique drivers of growth as a result of these use cases.[71] DLT applications to various fields, including financial transactions, Internet of Things (IoT), and value and supply chains, have grown exponentially. Blockchain 1.0 relied on proof-of-work (PoW) protocol as the foundation of blockchain technologies. From there, Blockchain 2.0 evolved to smart contracts involving greater functionality, decentralised applications, and autonomously executing algorithms. Blockchain 3.0 now focuses on larger-scale applications of non-currency-related DLT, improved performance, and greater scalability and interoperability, all rooted in proof-of-stake (PoS) protocol.[72]

As discussed above, the specificities of each DLT use case condition their challenges to the traditional notions of PIL. This section discusses PIL considerations in specific DLT use cases: tokenisation, digital currencies, cloud economies and metaverses, and decentralised autonomous organisations (DAOs).

4.1 *Tokenisation*

Applications of tokenisation today include asset tokenisation, non-fungible tokens (NFTs), global value and supply chains, and soulbound tokens (SBTs). Each of these classes of applications raise unique PIL considerations. This sub-section will brief discuss each class in turn.

4.1.1 Asset Tokenisation

Tokenisation of real assets refers to the digital representation of existing real (physical) assets on distributed ledgers,[73] including the representation on DLT of traditional asset classes such as financial instruments, collateral or real assets.[74] According to the OECD,

---

71 See in the field of security in the Internet of Things, *e.g.*, Anshul Jain, Tanya Singh, and Nitesh Jain, "Framework for Securing IoT Ecosystem Using Blockchain: Use Cases Suggesting Theoretical Architecture," in Milan Tuba, Shyam Akashe, and Amit Joshi (eds), *ICT Systems and Sustainability* (Springer 2020), 223–232.

72 "Proof of stake" refers to "a consensus distribution algorithm which determines which users are eligible to add new blocks to the blockchain, thus, earning a cryptocurrency payment as mining fee. Using this method, of the users who participate in the mining process, those with more tokens are favoured over those with less." See UNCTAD (n 2), 4 and 52.

73 Garrick Hilleman and Michel Rauchs, "2017 Global Blockchain Benchmarking Study," (*SSRN*, 21 September 2017), 51, 64 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3040224>.

74 See for example Financial Stability Board (FSB), "Decentralised financial technologies: Report on financial stability, regulatory and governance implications" (*FSB*, 6 June 2019) <https://www.fsb.org/wp-content/uploads/P060619.pdf>.

> [t]he application of DLTs and smart contracts in asset tokenisation has the potential to deliver a number of benefits, including efficiency gains driven by automation and disintermediation; transparency; improved liquidity potential and tradability of assets with near-absent liquidity by adding liquidity to currently illiquid assets; faster and potentially more efficient clearing and settlement. It allows for fractional ownership of assets which, in turn, could lower barriers to investment and promote more inclusive access by retail investors to previously unaffordable or insufficiently divisive asset classes, allowing global pools of capital to reach parts of the financial markets previously reserved to large investors.[75]

There are two types of asset tokenisation. The first is tokenisation that represents a pre-existing off-chain real asset. This type of asset tokenisation includes financial assets in conventional securities, non-financial assets such as real estate, and commodities such as gold. The second consists of tokens that are native to the blockchain, and which exist and trade only on-chain. This second type of asset tokenisation includes financial assets issued on DLT and equity securities.

Tokens representing a pre-existing off-chain real asset carry the rights of the assets that they represent. The real assets exist off-chain and are generally placed into safekeeping or custody to ensure that the tokens are constantly backed by the assets they represent. This type of tokenisation raises questions relating to the characterisation of such tokens for purposes of PIL,[76] and the significant role of custodianship of assets that have been tokenised.[77]

It is a truism that trust in the tokenisation of assets will depend on a credible central authority that can guarantee the connection of the real world with the blockchain. The regulation of tokenisation may be necessary to promote financial stability and market integrity while also protecting the consumer. Some experts have expressed the view that tokenisation simply replaces one digital

---

75 Organisation for Economic Co-operation and Development (OECD), "The Tokenisation of Assets and Potential Implications for Financial Markets" (*OECD*, 2020), 7 <https://www.oecd.org/finance/The-Tokenisation-of-Assets-and-Potential-Implications-for-Financial-Markets.pdf> accessed 15 December 2022.

76 For a discussion of the Swiss private international law applicable to various characterisations of tokens, see Chapter 22 of this book by Pascal Favrod-Coune and Kévin Belet, "Conflict of Laws and Tokens in Swiss Private International Law".

77 For an excellent discourse on possible connecting factors and policy choices, in particular in relation to asset tokenisation, see Ripley and Heindler (n 9).

technology with another – *i.e.,* a change from the use of electronic entries in securities registries of depositories with the use of cryptographic dematerialised securities based on DLT. As such, no issues of PIL, for example, in relation to jurisdiction, would arise if regulation were to take a technology-neutral approach.

On the other hand, given the novel nature of the models and processes involved in asset tokenisation, it may be unclear whether a domestic legal framework fully captures tokenisation. Legal frameworks put in place may need explicit jurisdiction over new actors, which will mostly be acting across borders. New regulation may also become necessary to regulate applicable law, jurisdiction, and recognition and enforcement in relation to the interoperability between the on-chain and off-chain habitats. Risks associated with the cross-border use of DLT, for example, in the cross-border management of financial risks and the cross-border protection of digital identity, may also need to be addressed. It has been noted that "[c]ross-border transactions of tokenised assets require international cooperation to limit regulatory arbitrage and for the smooth operation of tokenised markets".[78] This also includes dispute settlement, recourse and redress in case of fraud, insolvency, or technical fault.

Addressing the PIL issues that arise in asset tokenisation may become increasingly urgent as cross-border transactions of tokenised assets become more widespread.

4.1.2 Non-Fungible Tokens

Non-fungible tokens (NFTs) are a class of digital asset or token that can be proved to be unique, meaning that it is not interchangeable (*i.e.*, "non-fungible") with another digital asset token. The uniqueness, transparency and provability of ownership, and asset programmability of the NFT is usually cryptographically, immutably and publicly recorded on a distributed ledger.[79] This feature has been deployed to provide both digital and physical works with an NFT "certificate" of uniqueness and authenticity. The European Union Blockchain Observatory and Forum has noted that indicative NFT use cases include

78 *Id.* at 8.

79 The European Union Blockchain Observatory and Forum, "Demystifying Non-Fungible Tokens (NFTs)" (*EU BlockChain*, 20 November 2021), 4–5 <https://www.eublockchainforum.eu/sites/default/files/reports/DemystifyingNFTs_November%202021_2.pdf>.

digital art[80] (including gaming collectibles),[81] supply chain logistics,[82] content ownership,[83] and metaverse assets.[84]

Recent attention has focused on disputes arising from the minting, purchase, and theft of NFTs and NFT collections. For example, independent artists who post their work in publicly-viewable online galleries have reported that their artwork has been stolen and transformed into NFT collections without their consent.[85] These disputes indicate that challenges can arise based on the characterisation of NFTs (and whether they have proprietary status) and the lack of clarity over intellectual property rights (including copyright and trademark) associated with the token, especially when the token is linked with a physical good.

One PIL issue that arises in relation to NFTs is the recognition and enforcement of the underlying mechanism used for transferring and establishing ownership. Some commentators have argued that NFTs should be considered like property deeds that give an ownership title to a physical asset.[86] However, such deeds or titles generally entitle the holder to ownership of the asset but is not the asset in itself. In direct contrast, the purchase of an NFT gives ownership of the NFT itself, with any further rights

80 See, *e.g.*, Christie's, "Beeple, Everydays: The First 5000 Days" (*Christie's*) <https://onlineonly.christies.com/s/beeple-first-5000-days/beeple-b-1981-1/112924> accessed 15 December 2022, which was minted on 16 February 2021 and sold at online auction on 11 March 2021 in excess of USD 69 million.

81 See, *e.g.*, Cryptokitties, backed on the Ethereum blockchain, which allows players to breed digital kitties in-game to be traded via the use of NFTs.

82 See, *e.g.*, Nike's Cryptokicks project, for which it secured a patent, that stores unique identifiers given to each pair of shoes.

83 See, *e.g.*, Audius, "Home" (*Audius*) <https://audius.co/> accessed 15 December 2022, a decentralised audio streaming and sharing platform on the blockchain.

84 See, *e.g.*, for sales of digital land in the Sandbox and Decentraland, Keira Wright, "Virtual l and in the metaverse dominated NFT sales over past week" (*Cointelegraph*, 6 December 2021) <https://cointelegraph.com/news/virtual-land-in-the-metaverse-dominated-nft-sales-over-past-week>.

85 See, for example, Lois Beckett, "'Huge mess of theft and fraud:' artists sound alarm as NFT crime proliferates" (*The Guardian*, 29 January 2022) <https://www.theguardian.com/global/2022/jan/29/huge-mess-of-theft-artists-sound-alarm-theft-nfts-proliferates> and James Purtill, "Artists report discovering their work is being stolen and sold as NFTs" (*ABC*, 16 March 2021) <https://www.abc.net.au/news/science/2021-03-16/nfts-artists-report-their-work-is-being-stolen-and-sold/13249408>.

86 *Id.* at 40; see also Jeremy Goldman, "A Primer on NFTs and Intellectual Property" (*Lexology*, 11 March 2021) <https://www.lexology.com/library/detail.aspx?g=d96ed012-8789-4e87-bc1d-70ba76569c0f>.

or entitlements unless otherwise decided by the terms of the token smart contract. This raises the question of whether NFT transactions are solely contractual, or whether they carry proprietary characteristics. Other issues that arise in regard of characterisation is whether NFTs can be considered commodities[87] or securities.[88]

It should be noted that the proprietary nature of NFTs has been recognised in recent legal decisions rendered by the English and Singaporean courts.[89] Moreover, it has been noted that digital assets could be the subject of proprietary rights.[90] Consequently, the questions of whether digital assets are capable of infringing upon, conferring, or being protected under intellectual property rights has come to the fore.[91]

In addition, an NFT may also constitute a receipt of ownership for a linked real-world asset or a fraction of that asset, such as a portion of a digital painting.[92] In this regard there are risks associated with NFT trading, including poorly formed or non-existent contracts, unclear rights of ownership, and trademark and copyright concerns.[93] Notably, to overcome matters of enforcement relating to blockchain-based assets, a restraining order has been served via NFT.[94] The characterisation of NFTs—whether as property or not—is a pressing PIL issue that may merit further consideration.[95]

---

87 See, *e.g.*, the U.S. Commodity Futures Trading Commission (CFTC), "Digital Assets Primer" (*CFTC*, 2020) <https://www.google.com/url?sa=t&rct=j&q=&esrc> accessed 15 December 2022.

88 See, *e.g.*, the position of the U.S. Securities and Exchange Commission (SEC), "Framework for 'Investment Contract' Analysis of Digital Assets" (*SEC*, 2021) <https://www.sec.gov/files/dlt-framework.pdf> accessed 15 December 2022.

89 *Id*.

90 UNIDROIT, "Workshop on Issues Related to Enforcement in Digital Assets: Summary Conclusions" (*UNIDROIT*, 10 June 2022) <https://www.unidroit.org/wp-content/uploads/2022/08/Enforcement-and-DA-Side-Event-Draft-Summary-Conclusions-Final.pdf>. See also UNIDROIT's Draft Digital Assets Principles which includes guidance on linked digital assets, transfers relating to digital assets, custody of digital assets, secured transactions where digital assets were the collateral, and control over digital assets.

91 Amy Madison Luo, "NFTs: A Legal Guide for Creators and Collectors" (*Coindesk*, 11 March 2021) <https://www.coindesk.com/policy/2021/03/11/nfts-a-legal-guide-for-creators-and-collectors/>.

92 CODIFI Conference, Emeric Prévost, "Digital Economy / Loi applicable: determination par actif, par système ou par transaction?" 13 September 2022.

93 CODIFI Conference, Ronald Sum, "Digital Economy / Blockchain-Based Dispute Settlement Mechanisms," 14 September 2022.

94 CODIFI Conference, Andrew Hinkes, "Digital Economy / Digital Assets Remedies," 15 September 2022.

95 CODIFI Conference, Hin Liu, "Digital Economy / Digital Assets Remedies," 15 September 2022.

4.1.3 Global Value and Supply Chains

Global value and supply chains are sectors in which DLT has potentially transformative and disruptive applications. The use of DLT could transit the global value and supply chains from linear models to circular global chains in which parties are simultaneously and concurrently interacting with each other, potentially in real-time. Some processes could become entirely automated. These developments could catalyse a move away from a network of bundles of bilateral contracts. The reconfiguration of global value and supply chains would raise questions relating to the applicable law, the role of contracts, and the impact of automation on allocation of liability.[96]

4.1.4 Soulbound Tokens (SBTs)

The introduction of Soulbound Tokens (SBTs) in May 2022 by Vitalik Buterin and co-authors describes a new class of tokenisation and digital assets.[97] SBTs are defined as publicly-visible, non-transferable tokens representing affiliations, memberships, and credentials, enabling a DLT wallet to act as an "extended resume" of the holder's activities as relationships.[98] Illustrations of SBT use cases include proof of attendance at a conference, recognition of extensive contributions to a charity, or extensive participation in the governance of DAOs. SBTs can also be used to model traditional financial systems and arrangements, with a lien-like SBT showing that the holder has an outstanding debt obligation. Conversely, a credit score-like SBT may show that the holder has consistently made payments on a loan.

SBTs may provide a digital method of representing a wallet holder's location, personal identification, or affiliations. They could thus provide indication of real-world identities, locations, places of business, and patterns of social or economic behaviour. Interestingly, these are facts that facilitate the application of traditional connecting factors in PIL. Further, users would be incentivised to voluntarily acquire more SBTs to signal the consistency and reliability of their performance of obligations. SBTs may thus overcome the challenges

96 CODIFI Conference, Teresa Rodriguez De Las Heras Ballell, "Digital Economy / Expanded Applications of DLT: Supply Chain," 14 September 2022.

97 E. Glen Weyl, Puja Ohlhaver, and Vitalik Buterin, "Decentralized Society: Finding Web3's Soul" (*SSRN*, 11 May 2022) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4105763>.

98 The term "Soulbound" is borrowed from massively multiplayer online games, where Soulbound equipment is typically rewarded for accomplishments of high complexity and time investment and is "bound" to the player's "soul" because it cannot be traded or sold to other players. The equipment therefore has reputational value because it proves that the owner accomplished a significant challenge in the game.

that DLT poses to the PIL factors of *situs* and identity while respecting the ethos of peer-to-peer exchange that guides many DLT communities.

On the other hand, SBTs may challenge traditional notions of control under property law. SBTs are not intended to be freely transferable after initial acquisition, and users may only "destroy" it.[99] This may raise questions as to whether they may be accurately characterised as property. SBTs may thus raise complications in the search for general rules to characterise DLT assets.

4.2 *Digital Currencies*

Digital currencies are a "digital version of cash, controlled by a private cryptographic key – a unique random string of numbers."[100] Digital currency is owned by the holder of the private key associated with the relevant crypto wallet, which is used to hold and transfer the currency. There are currently three types of digital currencies: Central Bank Digital Currencies (CBDCs), which are digital versions of fiat issued by a country's central bank; Stable-Coins (*e.g.* Diem, formerly Libra), which are backed by a reserve asset such as fiat currency[101] held at banks; and Cryptocurrencies (*e.g.* bitcoin, ethereum, solana).

4.2.1 Central Bank Digital Currencies (CBDCs)

Token-based CBDCs have been defined as (a) a form of money (b) issued by a central bank (c) whereby the monetary claim on the central bank is incorporated in a digital token and (d) the transfer of the token equals transfer of the claim, (e) without current-account relationship between the central bank and the holder.[102] CBDCs have gained the attention of governments for their potential as a "new form of money"[103] to promote policy goals including financial

99 The hypothetical disincentive to doing so is that a wallet devoid of SCRTs will appear as a new user with no reputational markers, *i.e.*, potentially risky to transact with.

100 Visa (2021), "The Crypto Phenomenon: Consumer Attitudes & Usage", p. 7, available at https://usa.visa.com/content/dam/VCOM/regional/na/us/Solutions/documents/the-crypto-phenomenon-technical-paper.pdf.

101 "Fiat currency" refers to "any legal tender designated and issued by a central authority that people are willing to accept in exchange for goods and services because it is backed by regulation and because they trust this central authority." Consultative Group to Assist the Poor (CGAP), "Bitcoin versus Electronic Money" (*World Bank*, January 2014), 1 <https://documents1.worldbank.org/curated/en/455961468152724527/pdf/881640BRI0Box330WLEDGENOTES0Jan02014.pdf> accessed 15 December 2022.

102 Marianne Bechara et al. (eds), *IMF Fintech Note, Private Law Aspects of Token-Based CBDC* (First Draft, on file with author), para. 3.

103 *Id.* at para. 9. As opposed to account-based CBDC, token-based CBDC have been recognised to legally represent a truly "new form of money" that, per its definition, incorporates

inclusion; reduced transaction costs; resilience of payments in emergency situations; reduced illicit use of money; and increased competition in a country's payments sector.[104]

CBDCs have redefined the questions to be considered in the matter of the legal frameworks and developments that would need to be in place to reliably accommodate digital versions of fiat currency.[105] PIL questions that could arise include the recognition and enforcement of judgments in CBDC systems, jurisdiction in relation to intermediaries, and interoperability with existing (fiat) financial systems. CBDC trials are underway in jurisdictions like the People's Republic of China and the Bahamas, with expectation that they could be used in the future for cross-border payments, e-commerce, machine-to-machine transactions, and smart contracts. A PIL framework may need to be developed now rather than waiting until CBDCs have been put into actual practice. Additionally, legal frameworks concerning insolvency,[106] data protection and cyber security will need to be developed.[107]

The first PIL concern will be the characterisation of CBDCs. Determining the legal nature of CBDCs under existing property law classifications will bear on whether and how ownership rights in CBDCs can be held and evidenced.[108] This, in turn, will determine how CBDCs can be legally transferred between economic agents, held in custody and "deposited" with financial intermediaries, and pledged with creditors.[109] The legal roles of registries and wallets will also need consideration in order to determine the downstream implications on the holding and evidencing of ownership rights. Even if existing private international rules are to be applied to CBDCs, it is not clear whether the existing rules are fit for purpose.[110] If a CBDC is classified as a tangible-intangible hybrid under a domestic legal framework, for example,

---

a monetary claim on the central bank in a digital token where the transfer of that token equals transfer to the claim and that entails no current-account legal relationship between the central bank and the holder.

104 Gabriel Soderberg et al. (eds), *Behind the Scenes of Central Bank Digital Currency: Emerging Trends, Insights and Policy Lessons* (IMF 2022), 6–7.

105 *Id.*

106 For a discussion on private international law questions related to CBDCs, see Chapter 12 of this book by Caroline Kleiner, "The Law(s) Applicable to Central Bank Digital Currencies".

107 CODIFI Conference, Heng Wang, "Digital Economy / Central Bank Digital Currencies (CBDCs) & Private International Law," 13 September 2022.

108 Bechara et al. (n 103), para. 23.

109 *Id.* at para. 14.

110 *Id.* at para. 55.

the *lex rei sitae* could apply, but it is unclear what the *situs* of the distributed registers and wallets holding the CBDC tokens would be.[111]

In relation to cross-border CBDC access by non-residents, central banks may delegate functions to private sector intermediaries.[112] Banks examining and piloting CBDCs have converged on a model that is based on intermediation,[113] which may potentially require the use of foreign intermediaries, or intermediaries with worldwide offices. Some experts have thus argued that the PIL implications of these operations resemble the intermediation and dematerialisation challenges that informed the development of the *Convention of 5 July 2006 on the Law Applicable to Certain Rights in Respect of Securities held with an Intermediary* (HCCH 2006 Securities Convention).[114]

4.2.2 Stablecoins

There are three main categories of stablecoins: currency-linked stablecoins, asset-linked stablecoins, and stablecoins linked to cryptocurrencies or algorithms. In relation to stablecoins, it is important to note the fundamental distinction between the law that applies to the stablecoin, and the law that applies to the assets represented by the stablecoin. While parties are free to choose the law applicable to their contractual relationship in line with the principle of party autonomy, some comentators have argued that the freedom of choice of law must be limited to the stablecoin as such and should not extend to underlying assets that are themselves subject to mandatory PIL.[115]

The law applicable to assets represented by the stablecoin should be determined on the basis of the kind of asset represented by the token. However, the relationship between the stablecoin and the asset it represents is very tenuous. At present there is no consensus on which law should apply to that relationship, as it seems to fall between the cracks of the law governing the stablecoin and the law governing the asset represented by the stablecoin. An important PIL question is whether an asset that is part of stablecoin portfolio

111 *Id.*

112 See generally Bank for International Settlements (BIS), "Options for access and interoperability of CBDC for cross-border payments: Report to the G20" (*BIS*, July 2022) <https://www.bis.org/publ/othp52.pdf> accessed 15 December 2022.

113 Soderberg et al. (n 105), 8.

114 CODIFI Conference, Angelina Kwan, "Opening of the HCCH Securities Convention Track," 12 September 2022.

115 See, on this point, Chapter 13 of this book by Matthias Lehmann and Hannes Meyle, "The Law Applicable to Stablecoins".

must be distinguished from the law governing the stablecoin on the one hand and the assets of the portfolio on the other.[116]

4.2.3 Cryptocurrencies

Cryptocurrencies have been the subject of intense scrutiny over the last few years.[117] Specifically, specific objections have been raised to the application of PIL frameworks to legal relationships involving the use of cryptocurrencies. These objections have either been based on the argument that these relationships are self-regulated and are subject to the *lex cryptographica* as opposed to legal regulation such as *lex mecatoria*,[118] or that there are major obstacles to the application of PIL to cryptocurrencies, including the delocalisation of transactions and the pseudonymity of actors.[119] These objections have been framed along two lines – either by classing cryptocurrencies as assets in the sense of intangible movable property or by viewing cryptocurrencies as currency, and applying PIL by analogy.[120] The rapid evolution and diversification of the crypto asset and cryptocurrency landscape will require that choice of law rules offer "a sufficient degree of flexibility along with legal foreseeability and certainty".[121] One possible solution may be to allow for the principle of party autonomy in choice of law.[122] This would allow parties to agree on the law governing the relationship between them, while accepting that there may be certain limitations on the freedom of choice.[123]

---

116 *Id.*

117 On a range of approaches and challenges dealing with cryptocurrency in the private international law, see Chapter 11 of this book by Francesca C. Villata, "Cryptocurrencies and Conflict-of-Laws"; see also CODIFI Conference, Andrew Hinkes, "Digital Economy / Digital Assets Remedies," 15 September 2022.

118 See, *e.g.*, Primavera De Fillippi and Aaron Wright, *Blockchain and the Law – The Rule of Code* (HUP 2018). For an opposite view, see Chapter 4 of this book by David Sindres, "Is Bitcoin out of Reach for Private International Law?".

119 See, *e.g.*, Mathias Audit, "Le droit international privé confronté à la blockchain," (2020) 4 Revue critique de droit international privé 669, 689.

120 See, *e.g.*, Sindres (n 119).

121 Ripley and Heindler (n 9).

122 Symeon C. Symeonides, *Codifying Choice of Law Around the World: An International Comparative Analysis* (OUP 2017), Chapter 3.

123 See, *e.g.*, HCCH (n 10), Annex I.

4.3 *Cloud Economies and Metaverses*

Cloud economies and web3 metaverses are "emerging market virtual world economies with a continually developing complex mix of digital goods, services, and assets that generate real-world value for users".[124] They allow users to own and trade digital assets as NFTs, creating a "new free-market internet-native economy that can be monetised in the physical world".[125] Examples of commercial activities in cloud economies and metaverses include art galleries,[126] business headquarters,[127] sponsored content,[128] and music venues.[129] The metaverse has been described as a high-revenue opportunity that spans social commerce, digital events, hardware, and content monetisation.[130]

Cloud economies and metaverses are use cases for Decentralised Finance (DeFi), including aggregators, DeFi primitives, oracles, and marketplaces. They work with agents relating to sovereign virtual goods and NFTs, including minting houses, metadata and token standards, as well as physically redeemable NFTs. The characterisation of these agents will have an impact on the PIL implications of the applicable legal frameworks. Of particular significance to PIL considerations is that fact that cloud economies and metaverses involve decentralised governance, including DAO frameworks and their attendant voting mechanisms, community audits, and multisignature wallets.[131] The decentralised

---

124 David Grider, "The Metaverse: Web 3.0 Virtual Cloud Economies" (*Grayscale*, November 2021), 10 <https://grayscale.com/wp-content/uploads/2021/11/Grayscale_Metaverse_Report_Nov2021.pdf> accessed 15 December 2022.

125 *Id.* at 7.

126 See, *e.g.*, "Salgado" (*Sotheby's*) <https://metaverse.sothebys.com/salgado> accessed 15 December 2022.

127 See, *e.g.*, "Markets" (*Binance*) <https://www.binance.com/en/markets/coinInfo-Metaverse> accessed 15 December 2022.

128 See, *e.g.*, "DCL x Atari: Yes, you read that correctly – Atari is coming to Decentraland" (*Decentraland*, 26 January 2021) <https://decentraland.org/blog/announcements/dcl-x-atari/>.

129 See, *e.g.*, Travis Scott, "Travis Scott and Fortnite Present: Astronomical (Full Event Video)" (*YouTube*, 26 April 2020) <https://www.youtube.com/watch?v=wYeFAlVC8qU>, Kizuna AI, "Introduction" (*2020hello*) <https://2020hello.world/en/> accessed 15 December 2022, and Kai from Splash, "About" (*Virtual Humans*) <https://www.virtualhumans.org/human/kai> accessed 15 December 2022.

130 Grider (n 125), *op. cit.* (n 115), 9, 16. See also Pedro Palandrani, "The Metaverse Takes Shape as Several Themes Converge" (*Global X*, 13 September 2021) <https://www.globalxetfs.com/content/files/The-Metaverse-Takes-Shape-as-Several-Themes-Converge.pdf>.

131 A "multisignature wallet" (also referred to as a "multigeniture wallet") refers to a cryptocurrency wallet that requires authentication from multiple parties to complete a transaction, which is the type of cryptocurrency wallets commonly used in DAOs, see, *e.g.*, Monika di Angelo and Gernot Salzer, "Characteristics of Wallet Contracts on Ethereum"

cloud services implicated means that storage, computing, and databases are decentralised in the borderless cloud. The borderless nature of cloud economies and metaverses creates challenges for the traditional significance of geographic location in PIL.[132]

Another issue that arises in cloud economies and metaverses is the PIL implications of cross-border data transactions. PIL questions relating to jurisdiction, applicable law and recognition may become increasingly urgent as data transactions take place in the cloud economy, and as certifications of data transactions are increasingly tokenised.

One PIL issue that arises in cross-border data transactions is the question of characterisation. UNCITRAL's work related to data transactions has found that contracts for the provision of data are analogous to contracts for the sale of goods, whereas contracts for the processing of data are analogous to contracts for services.[133] This may have an impact on the determination of the applicable law. It may be significant to note that UNCTAD's position is that that cross-border data flows are distinct from both goods and services and should be considered neither e-commerce nor trade.[134] These divergent approaches to the characterisation of cross-border data flows may have implications on the development of a PIL framework for cross-border data transactions in cloud economies and metaverses.

It has been noted that determining the applicable law in cloud economies and metaverses is increasingly important, and perhaps should be regulated by an international treaty.[135] Potential issues include due process, incapacity, or the award being contrary to public policy.[136] The creation of specific solutions relating to jurisdiction, applicable law, and enforcement of metaverse-related disputes may, however, need to be based on the specific contours of the

(*TU Wien*), 1–2 <https://publik.tuwien.ac.at/files/publik_289326.pdf> accessed 15 December 2022.

132 Dan Jerker B. Svantesson, "The (uneasy) relationship between the HCCH and information technology," in Thomas John, Rishi Gulati, and Ben Kohler (eds), *The Elgar Companion to the Hague Conference on Private International Law* (Edward Elgar Publishing 2020), 462.

133 UNCITRAL, "Legal issues related to the digital economy (including dispute resolution) – progress report" (*UNCITRAL*, 5 April 2021), 4–5 <https://uncitral.un.org/sites/uncitral.un.org/files/1064_advance_copy_e.pdf>.

134 UNCTAD, "Digital Economy Report 2021 Overview" (*UNCTAD*, 29 September 2021), 3–5 <https://unctad.org/system/files/official-document/der2021_overview_en_0.pdf>.

135 CODIFI Conference, Juliette Asso, "Digital Economy / Expanded Applications of DLT: Metaverses," 14 September 2022.

136 CODIFI Conference, Juliette Asso and Laura Azaria, "Digital Economy / Expanded Applications of DLT: Metaverses," 14 September 2022.

metaverse. Some experts have opined that the use of a metaverse to carry out a transaction is sufficient to make the transaction international, making each transaction subject to the relevant conflict of laws applicable.[137]

Moreover, it should be noted that metaverses are decentralised, dematerialised, virtual worlds in which anonymous avatars transact.[138] An expert has noted that off-chain enforcement raises important PIL concerns relating to pseudonymity and the question of where recognition and enforcement proceedings of a transaction carried out in a metaverse should be initiated.[139] In this regard, guidelines and rules that allow for some cross-border certainty and harmonisation between jurisdictions may be helpful.[140]

4.4 *Decentralized Autonomous Organisations* (*DAOs*)

The difference between regulated DAOs incorporated under the law of a State and "maverick DAOs" lacking any such framework underlie questions relating to PIL.[141] These questions concern (a) whether regulated DAOs can be recognised in other States; (b) whether maverick DAOs have a legal existence in State jurisdictions; and (c) what law could be applicable to a maverick DAO. DAO compliance with securities laws, and whether distributions from a DAO cooperative may have tax consequences, are topics on which clarity in PIL matters would be helpful.[142]

Some experts have proposed that one possible way forward would be the development of a PIL convention framework that would address the law applicable to DAOs. This convention could provide a framework for the automatic recognition of DAOs that have been validly incorporated, constituted

137 *Id.*

138 CODIFI Conference, Juliette Asso, "Digital Economy / Expanded Applications of DLT: Metaverses," 14 September 2022.

139 CODIFI Conference, Laura Azaria, "Digital Economy / Expanded Applications of DLT: Metaverses," 14 September 2022.

140 *Id.*

141 CODIFI Conference, Florence Guillaume and Sven Riva, "Digital Economy / Decentralised Autonomous Organisations," 15 September 2022. For an excellent exposition on the structure and functioning of DAOs, including the separation between "regulated" and "maverick" DAOs, see Chapter 20 of this book by Florence Guillaume and Sven Riva, "Blockchain Dispute Resolution for Decentralized Autonomous Organizations: The Rise of Decentralized Autonomous Justice".

142 CODIFI Conference, James Wigginton, "Digital Economy / Decentralised Autonomous Organisations (DAOs)," 15 September 2022.

or organised.[143] This recognition of a DAO must include the recognition of its legal personality and the limited liability of its members, so that DAOs can be utilised as legal vehicles for businesses.[144] Methods to determine the possible applicable law may rely on the code of the DAO or resort to rules of law that are generally accepted on an international level.[145]

5 Role of PIL Harmonisation in DLT – Why Harmonise?

Initiatives to better frame the legal framework around DLT have been undertaken, with varying degrees of complexity and speed, by regulators around the world. The heterogeneity of these various regulatory initiatives has raised concerns about the implications for PIL, in particular a concern about fragmentation in approaches relating to applicable law, choice of law, choice of forum, recognition, and enforcement. For example, Germany elaborates on such concerns in its *Blockchain Strategy of the Federal Government*, which includes the matter of which legal system applies, as well as the issue of the enforceability of law in cross-border DLT structures.[146]

Fragmentation can already be observed at different levels. First, not all kinds of digital assets available are regulated. In many jurisdictions, only some of them (mostly cryptocurrencies) have been the object of domestic frameworks.[147] Other jurisdictions have addressed specific DLT applications.[148] Still others have approached the matter from the angle that there is a need to regulate the digital economy more broadly.[149] Moreover, the use and understanding of terminology are varied among the different initiatives. Second, in relation to the assets regulated, the legal nature of the assets has been understood differently by different jurisdictions. For example, some jurisdictions classify

143 CODIFI Conference, Florence Guillaume, "Digital Economy / Decentralised Autonomous Organisations (DAOs)," 15 September 2022.

144 CODIFI Conference, Sven Riva, "Digital Economy / Decentralised Autonomous Organisations (DAOs)," 15 September 2022.

145 CODIFI Conference, Florence Guillaume, "Digital Economy / Decentralised Autonomous Organisations (DAOs)," 15 September 2022.

146 German Federal Ministry for Economic Affairs and Climate Action and Ministry of Finance, "Blockchain Strategy of the Federal Government: We Set Out the Course for the Token Economy" (*BMWK*, 7 March 2019) <https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/blockchain-strategy.pdf?__blob=publicationFile&v=3>.

147 See more details per country in HCCH (n 10), Annex II.

148 See the examples of Bermuda and Mauritius in *id.*

149 See the examples of Liechtenstein and Switzerland in *id.*

cryptocurrencies as equivalent to securities, and apply the relevant securities laws and regulations.[150] Other jurisdictions consider cryptocurrencies to be property or fungible assets, and apply the relevant property law.[151] Third, the fragmentation can be also observed in terms of the different approaches taken towards legal reform aimed at regulating the emerging digital economy. While some jurisdictions have issued papers pointing towards the continuing applicability of existing legal frameworks,[152] other jurisdictions have amended their legislations or issued new legislation.[153]

A recent mapping initiative from the Global Blockchain Business Council, the Global Standard Mapping Initiative (GSMI) 2020, emphasised the need for uniform global standards to facilitate impactful and responsible cross-border innovation in relation to DLT.[154] The Report, which represented an "unprecedented effort to map and analyse the current blockchain landscape", noted the fragmentation of regulatory approaches across the world, and that "existing efforts to coordinate across jurisdictions have been piecemeal at best and chaotic at worst".[155] The Report concludes "breaking through traditionally siloed bodies of information, industries, and geographic barriers will facilitate more functional networks".[156]

Fragmentation creates challenges for the digital economy, which is inherently cross-border. A uniform PIL framework can address such challenges without interfering with the internal regulation of these decentralised systems, thereby providing coherence and certainty to the relevant stakeholders while domestic initiatives are ongoing.[157] A harmonised PIL framework based on generally acceptable conflict-of-laws principles will thus protect users (and especially ensure weaker party protection), enable innovation, improve good governance, and strengthen the rule of law in the digital economy.[158] Specific concerns arise in the fields of insolvency and intellectual property.

---

150 See the examples of Australia, Israel, Kazakhstan and Singapore in *id*.

151 See the examples of the People's Republic of China and Italy in *id*.

152 See the examples of Australia, Israel, Lithuania and the United Arab Emirates in *id*.

153 See the examples of Bermuda, France, Liechtenstein, Mauritius, Singapore and Switzerland in *id*.

154 Global Blockchain Business Council (GBBC), "Global Standard Mapping Initiative (GSMI) 2020" (*GBBC*, October 2020), 2 <https://gbbcouncil.org/wp-content/uploads/2020/10/GSMI-Legal-Regulatory-Report.pdf>.

155 See (n 145), 25.

156 *Id.*

157 CODIFI Conference, Hin Liu, "Digital Economy / Digital Assets Remedies," 15 September 2022.

158 CODIFI Conference, Louise Gullifer, "Digital Economy / Characterising Relationships Between Asset Holders and Exchanges," 21 September 2022.

In relation to insolvency, UNCITRAL Working Group V: Insolvency Law (UNCITRAL WG V) is currently considering applicable law in insolvency proceedings. The UNCITRAL Secretariat noted that "rules for localisation of assets, law applicable to the rights and claims existing at the time of the commencement of insolvency proceedings … or other rules of private international law" may be outside the scope of UNCITRAL WG V's study, and that these matters could "become the subject of a separate study that would need to be undertaken in close cooperation with the Hague Conference on Private International Law".[159] At the HCCH's recently concluded CODIFI Conference, expert discussions highlighted a number of cross-border issues concerning insolvency and digital transactions and assets, such as third-party effects of insolvency of digital asset platforms, the characterisation of digital assets as property for the purposes of an insolvency proceeding, and the mechanics of injunctive relief involving electronic platforms.[160]

In relation to the protection of intellectual property rights, experts have noted that DLT systems and applications have given rise to a wide range of implications in the field of intellectual property.[161] The advent of the digital economy and DLT systems and applications has motivated study of whether existing instruments and legislation are adequate for the new technological landscape. Experts thus have proposed an approach that leverages pre-existing connecting factors, with adaptations being made to apply to situations involving the protection of intellectual property rights relating to DLT applications or crypto assets.[162] Existing rules may thus need to be updated through legislative action or by the judiciary, as necessary. The HCCH is continuing with its monitoring of intellectual property-related developments and cases in the digital sphere, and in particular the emerging proliferation of litigation over digital collectibles. The jurisprudence in this regard illustrates that there is confusion over the technical and legal underpinnings of NFTs and the properties and rights that may be linked to them. Until a uniform international perspective

159 *Id.*

160 For a detailed discussion of international insolvency law in relation to cryptocurrencies, the (proprietary or contractual) relationships involved between exchanges and users, and jurisdiction and applicable law questions in insolvency proceedings concerning cryptocurrencies, see Chapter 15 of this book by Giovanni Maria Nori and Matteo Girolametti, "International Insolvency Law and Cryptocurrencies".

161 CODIFI Conference, Florian Heindler, "Digital Economy / PIL & DLT: What Challenges Lie Ahead?," 15 September 2022.

162 *Id.*; CODIFI Conference, Andrea Bonomi, "Opening of the Digital Economy 'Frameworks' Track," 12 September 2022.

emerges in this regard, the PIL implications of domestic regulatory approaches to intellectual property remains pressing.

6 Prospects for the Harmonisation of PIL in DLT

Work is ongoing at the HCCH, UNCITRAL and UNIDROIT in relation to the harmonisation of PIL in DLT-related sectors.[163] These three sister organisations are committed to cooperatively explore and respond to the intersection of technology, economics, and law found in DLT. The digital economy, including DLT-based applications, is a topic where the work of all three organisations is converging.[164] Each of these organisations has received requests from their members to study and provide guidance on different aspects of the topic. Coordination between the three organisations is thus important to ensure proper harmonisation but is also challenging given the rapid pace at which the landscape of DLT-based applications continues to shift.[165]

UNCITRAL has continued to work on five key topics: Artificial Intelligence and automation, Data transactions, Digital assets, Online platforms and specifically, Distributed ledger systems and technology. DLT-based applications run through these five topics, and UNCITRAL has emphasised the importance of coordination with the HCCH on the PIL aspects identified in this work.[166] The HCCH participates as an observer in UNCITRAL's Working Group IV on Electronic Commerce and Working Group V on Insolvency.

UNIDROIT continues its work on the development of a set of Principles by their Working Group on Digital Assets and Private Law, which include a Principle on PIL. The HCCH participates as an observer in this work, and UNIDROIT has noted that the input of the HCCH continues to be welcome in the development of this Principle on PIL.[167]

The HCCH has, since March 2020, allocated resources to follow the PIL implications relating to developments in the field of DLT, in particular in

163 CODIFI Conference, Christophe Bernasconi, Anna Joubin-Bret, and Ignacio Tirado, "CODIFI – Tripartite Discussion: HCCH, UNCITRAL, UNIDROIT," 12 September 2022.

164 CODIFI Conference, Gérardine Goh Escolar et al., "Digital Economy / Closing Session: Concurrent Design Facility," 16 September 2022.

165 *Id.*

166 CODIFI Conference, Anna Joubin-Bret, "CODIFI – Tripartite Discussion: HCCH, UNCITRAL, UNIDROIT," 12 September 2022.

167 CODIFI Conference, Ignacio Tirado, "CODIFI – Tripartite Discussion: HCCH, UNCITRAL, UNIDROIT," 12 September 2022.

relation to FinTech.[168] Under the mandate given to it by its Council on General Affairs and Policy, the HCCH recently concluded the inaugural HCCH Conference on Commercial, Digital and Financial Law Across Borders (CODIFI Conference).[169] The CODIFI Conference sessions were organised along six thematic tracks, including three tracks that address matters related to the digital economy and, more specifically, DLT. Topics selected for these three tracks were informed by the requests of Members which had responded to a survey distributed by the Permanent Bureau in late 2021.

- The Digital Economy "Frameworks" track focused on the PIL issues in the new decentralised economy that is based on technologies such as DLT;
- The Digital Economy "Relationships" track considered the use of DLT and other technologies as building blocks for governance of enterprises, transactions, financial services, dispute resolution, operations management and sustainable development; and
- The Digital Economy "Redefine" track broadly considered innovations in the fintech industry, including specific perspectives and approaches of national jurisdictions regarding digital commerce.

At the time of writing, the outcomes of the HCCH CODIFI Conference have been compiled to inform Members of the HCCH in preparation for their next CGAP meeting in March 2023, at which the Members will decide on the future work programme of the HCCH. Based on the findings and recommendations of the experts who participated in the HCCH CODIFI Conference, HCCH Members may consider further work on the harmonisation of private international law rules in relation to the digital economy more broadly, and the applications that include those based on DLT more specifically.

7 Conclusion: Looking to the Future

Recent strides made in the growth and mainstreaming of Web3 have been powered by the token and DLT-based economy, and its "potential to revolutionize

168 HCCH "Proposal for the Allocation of Resources to follow Private International Law implications relating to Developments in the field of Distributed Ledger Technology, in particular in relation to Financial Technology" (*HCCH*, March 2020) <https://assets.hcch.net/docs/f787749d-9512-4a9e-ad4a-cbc585bddd2e.pdf> accessed 15 December 2022.

169 See for more information, HCCH, "HCCH CODIFI Conference" (*HCCH*) <https://www.hcch.net/en/projects/post-convention-projects/hcch-codifi-conference> accessed 15 December 2022.

agreements and value exchange".[170] Web3 is defined by various parties as the "Read-Write-Own"[171] internet "owned by its builders and users, and orchestrated with tokens".[172] Forecasts are that this new user-owned economy will, in the long-term, outperform the traditional economy based on legacy institutions.[173]

In the digital trade sector, the complexity of cross-border transactions, including those based on DLT, continues to pose challenges in the discernment of applicable rules amidst different domestic legal systems.[174] Emerging technologies have altered the way in which regulatory authorities, businesses and consumers conduct transactions and resolve disputes. Issues of computational law and digitalisation may lead to silos between diverse actors and commercial systems, including "hard" and "soft-law" instruments, being broken.[175]

The digital economy, including that based on DLT, has documented benefits in terms of job creation, and the empowerment of women and minorities. It also provides regulatory sandbox opportunities to validate innovations. However, extensive cross-border cooperation to achieve harmoniation and support the adoption of common minimum standards may be timely and necessary.[176] A robust and harmonised PIL framework will ensure the legal certainty necessary to allow the transition towards a more sustainable economy, while protecting consumers and weaker parties, and provide a useful framework in the achievement of Environmental, Social and Governance (ESG) initiatives and risk management. The legal certainty ensured by a harmonised PIL framework will support greater financial inclusion by enabling greater access to modern financial services and financing.[177]

---

170 Shermin Voshmgir, *Token Economy: How the Web3 Reinvents the Internet* (2nd edn, BlockchainHub Berlin 2020), 2.

171 Eshita, "Web3: in a nutshell" (*eshita.mirror.xyz*, 9 September 2021) <https://eshita.mirror.xyz/H5bNIXATsWUv_QbbEz6lckYcgAa2rhXEPDRkecOlCOI>.

172 Chris Dixon, "Why Web 3 Matters" (*Twitter*, 26 September 2021) <https://twitter.com/cdixon/status/1442201621266534402>.

173 See, *e.g.*, Jason Potts and Ellie Rennie, "Web3 and the creative industries: How blockchains are reshaping business models," in Stuart Cunningham and Terry Flew (eds), *A Research Agenda for Creative Industries* (Edward Elgar Publishing 2019), 93–111.

174 CODIFI Conference, Craig Atkinson, "CODIFI – Digital Economy / Human-Centred Finance and Trade for Sustainable Development," 16 September 2022.

175 *Id.*

176 CODIFI Conference, Laurence Thébault, "CODIFI – Digital Economy / Human-Centred Finance and Trade for Sustainable Development," 16 September 2022.

177 *Id.*

PART 1

Fundamental Questions

CHAPTER 2

Technical Description of DLT for Conflicts Lawyers

Tetsuo Morishita

1 Purpose of this Chapter

The purpose of this chapter is to examine the basics of Distributed Ledger Technologies ("DLTs") as well as the typical use cases of DLTs.

Conventional Private International Law (PIL) has typically used the approach of determining the applicable law by determining, through connecting factors, the country where the relationship has its center of gravity (situs) or to which it is most closely connected. Needless to say, in deciding to which country the relationship is most closely connected, it is necessary to have an accurate understanding of the reality of the relevant facts. This chapter first examines three key technical elements of blockchains: block and chain structure, peer-to-peer and consensus algorithm, and cryptography as well as the distinction between permissionless and permissioned blockchain. Next, some use cases of blockchain and possible disputes are illustrated.

Distributed Ledger Technology ("DLT") is a technology that keeps records across a set of devices (typically, PCs and smartphones) in a network, which are called "nodes," so that the records are synchronised between nodes using a consensus mechanism.[1] The most well-known example of DLTs is the blockchain. Though the blockchain is one application of DLT, it is not the only

1 For example, a report issued by the World Bank Group explains, "DLT refers to a novel and fast-evolving approach to recording and sharing data across multiple data stores (ledgers), which each have the same data records and are collectively maintained and controlled by a distributed network of computer servers, which are called nodes." (World Bank Group, "Distributed Ledger Technology (DLT) and Blockchain (FinTech Note No.1)" (*World Bank Group*, 2017),1<https://openknowledge.worldbank.org/bitstream/handle/10986/29053/WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf> accessed 30 May 2022. The International Organization for Standardization issued ISO22739:2020 in 2020 as an initiative to define basic terms relating to blockchain and distributed ledger technologies. (International Organization for Standardization, *Blockchain and distributed ledger technologies – Vocabulary* (Switzerland: International Standard 2020) ("ISO22739")). In the ISO22739, a "distributed ledger" is defined as a "ledger that is shared across a set of DLT nodes and synchronized between the DLT nodes using a consensus mechanism." *Id.*, 3.22.

© TETSUO MORISHITA, 2023 | DOI:10.1163/9789004514850_004
This is an open access chapter distributed under the terms of the CC BY-NC-ND 4.0 license.

one.[2] Though, there are applications of DLT that do not apply the block structure, the following part of this chapter focuses on blockchain.

2 Key Elements of Blockchain

The ISO 22739 defines "blockchain" as "distributed ledger with confirmed blocks organised in an append-only, sequential chain using cryptographic links."[3] As this definition shows, blockchain has three key elements that differentiate it from conventional technologies.

2.1 *Block and Chain Structure*

The block structure is the first key element that differentiates blockchain from conventional technologies. In a blockchain, records are stored in blocks and connected like a chain. Each block consists of two parts: the block header and the record (see Figure 2.1). The block header typically is composed of the hash of the previous block's header, the timestamp, nonce (a number used to provide replay protection), and the Merkle root (the hash of all records in the block).[4] If the previous block is tampered with, the hash value will change, and the blocks will not connect correctly. Therefore, if one attempts to forge a record in the chain and tamper with one block, all blocks subsequent to that tampered block would have to be recreated, which is difficult to do in practice. Therefore, the system is resistant to tampering and is suitable for recording the entire history of transactions. In addition, as a result of such a blockchain structure, the record can be added to the chain in time-sequential order, and once a record is added to the chain, it is almost impossible to change the record.[5]

2 Regarding the difference between DLT and blockchain, see Ayushi Abrol, "Blockchain Vs. Distributed Ledger Technology" (*Blockchain Council*, 11 March 2022) <https://www.blockchain-council.org/blockchain/blockchain-vs-distributed-ledger-technology/> accessed 4 April 2023.

3 ISO22739 (n 1), 3.6.

4 Imran Bashir, *Mastering Blockchain* (3rd edn, Packt Publishing 2020), 16–17. On the blockchain of Bitcoin, Primavera De Filippi and Aaron Wright, *Blockchain and the Law* (Harvard University Press 2018), 22–23.

5 Bashir (n 4), 13. One of the rare scenarios that the change of the record occurs is that someone who has got more than 51% of the power uses its power to alter the previous records. *Id.*

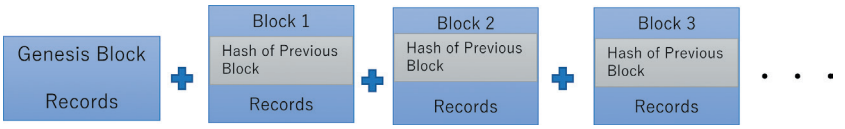

FIGURE 2.1 Mechanism of blockchain

When the blockchain is used for Bitcoin, the record on the blockchain shows the record of transactions between the addresses,[6] such that a certain amount of the digital asset is transferred from one address to the other address. However, no information about the current balance is held by the blockchain. So, when one wants to know the balance of the assets corresponding to the address, the amount is not available on the blockchain[7] and must be calculated from the transaction records (the amount that had been transferred to the address before a transaction minus the amount that has been transferred from the address).

There may be a situation in which a chain is divided into two or more chains, called a "fork." There are two types of forks. One is a "soft fork," which is a temporary fork due to a specification change of software (such as upgrade) or the reorganisation during regular operation. The other is a "hard fork," which is the result of the division of the developers' community, and in which the chain is divided into two completely different chains.[8] In case of soft fork, the previous blocks and the new blocks are both acceptable, while, in case of hard fork, previously valid blocks become invalid after the hard fork.[9] For example, the Bitcoin and Ethereum blockchains experienced hard forks in the past, resulting in different versions (e.g. Bitcoin Classic and Bitcoin; Ethereum Classic and Ethereum).

6 In the case of Bitcoin, the address is created by taking the corresponding public key of a private key and hashing it twice, usually 26–35 characters long. Bashir (n 4), 198.

7 One Japanese court case opined that records on the blockchain are only a history of transactions, and the lack of a record about the balance of the bitcoin for the corresponding bitcoin address is one of the reasons why bitcoin could not be the object of ownership rights under Japanese law. On this point, Stacey Steele, and Tetsuo Morishita, "Lessons from Mt Gox: practical considerations for a virtual currency insolvency," in Douglas W. Arner et al. (eds), *Research Handbook on Asian Financial Law* (Elgar 2020), 479, 492.

8 International Organization for Standardization, *Blockchain and distributed ledger technologies – Security management of digital asset custodians* (Switzerland: International Standard 2020), 9–10 (ISO/TR 23576).

9 Bashir (n 4), 218.

2.2 *P2P and Consensus Mechanisms*

The peer-to-peer network is the second key element that differentiates the blockchain from conventional digital storing technologies. In conventional recording systems, transaction data have been kept by some specified entities, and the entities have the power to add, delete or change the records. On the blockchain, in contrast, records are shared by nodes participating in the network, and new records are added according to a predetermined consensus mechanism. Sharing records by a wide range of nodes is said to contribute to making the blockchain resilient to failure and forgery because the failure or corruption of a node, for instance that is caused by hacking, would have little impact on the network as a whole; there are other nodes that continue to work and keep accurate records.[10] Also, sharing the same records by nodes in the network is said to result in increased transparency, because records are auditable by nodes that share the records.[11] However, such transparency is limited to information available from the records on the blockchain. Therefore, in the case of Bitcoin, no information about the person or entity that is connected to the Bitcoin address is available in the record on the blockchain, so there is no transparency regarding who, in the real world, has an interest in Bitcoin on the blockchain ("pseudonymity" or "anonymity"). Nodes performs various functions such as communicating data, validate transactions, perform mining, and providing wallet depending on the type of blockchain.[12] Also, there are types of nodes and not all nodes necessarily perform all these functions. Though there are several ways of categorization, nodes are typically divided into two categories. One is a "full node" that stores blockchain data and verifies all transactions. The other is a "lightweight node" or a "simple payment

10 Filippi and Wright (n 4), 35–37. However, it should be noted that such resiliency may depend on the number and location of nodes. In case of permissionless blockchain, the number of nodes could be many. For example, Bitcoin has more than 10,000 active nodes (Osato Avan-Nomayo, "Bitcoin network node count sets new all-time high" (*Cointelegraph*, 15 July 2021) <https://cointelegraph.com/news/Bitcoin-network-node-count-sets-new-all-time-high> accessed 29 June 2023). On the other hand, in a permissioned blockchain, the number of nodes is more limited. If the number of nodes is limited and such nodes are closely located, most nodes may be damaged at the same time by some natural disaster in the location. On the other hand, the distance between nodes may affect the speed of communication. Study Group on Law and Technology Relating to Blockchain, "Possibilities and Issues of Blockchain – Dialogue between Law and Technology" (2017) 2076 Kinyu Homu Jijou 6, 12–13 (Japanese: *Blockchain nikansuru Ho to Gijutsu Kenkyukai,* "*Blockchain no Kanosei to Kadai – Ho to Gijutsu no Taiwa –*" (2017) 2076 Kinyu Homu Jijou 6, 12–13).

11 *Id.*, 37.

12 Bashir (n 4), 19.

verification node" that downloads only the headers of the block (the header is the smallest unit of the block), does not verify all transactions, and receives records from other full nodes when necessary. Full nodes are more secure because they can verify all transaction by themselves without relying on other nodes. However, they require large amount of storage and high uptime as well as technical knowledge, and most non-business users do not choose full nodes. On the other hand, lightweight nodes do not need much storage and can be run with devices of limited storage.[13] For this reason, lightweight nodes are more common. However, they need to connect to full nodes to interact with the blockchain network, and it is pointed out that there is a threat to privacy and security.[14]

The consensus mechanism is the mechanism for the distributed system to reach consent on the validity of the records. In blockchains, a consensus algorithm runs when blocks are appended to the existing chain of blocks.[15] In a distributed network such as blockchain, especially in a permissionless distributed network, in which nodes with malicious intention (so-called "Byzantine nodes") may not be excluded due to the network's open access, the consensus mechanism needs to overcome the presence of such Byzantine nodes.

There are various types of consensus mechanisms. The consensus mechanisms used in blockchains can roughly be divided into two categories:[16] "proof-based" and "byzantine fault tolerance."[17] The former is the mechanism electing a leader at random using an algorithm and may be used in permissionless

13 Coinbase, "Blockchain client types" (*Coinbase* 27 January 2022) <https://www.coinbase.com/ja/cloud/discover/dev-foundations/blockchain-client-types> accessed 16 April 2022; Nodes, "Blockchain Nodes: An In-depth Guide" (*Nodes*) <https://nodes.com/#blockchain-nodes-types> accessed 16 April 2022.

14 Lin Ge and Tao Jiang, "A Privacy Protection Method of Lightweight Nodes in Blockchain" (2021) 2021 Security and Communication Networks 1.

15 WisdomTree Market Insight, "Consensus Mechanism Overview" (*WisdomTree Market Insight*, August 2021) <https://www.wisdomtree.eu/en-en/-/media/eu-media-files/other-documents/research/market-insights/wisdomtree_market_insight_consensusmech_en.pdf> accessed 29 June 2023.

16 Bashir (n 4), 31.

17 The word "byzantine" comes from the famous "Byzantine generals problem." The problem is illustrated by the following situation: Several divisions of the Byzantine army commanded by its own general are camped outside an enemy city. The generals can communicate with one another only by messenger. They must decide upon a common plan of action against the enemy. However, some of the generals may be traitors, trying to prevent the loyal generals from reaching agreement. The generals must have a mechanism to guarantee (i) all loyal generals decide on the same plan of action and (ii) a small number of traitors cannot cause the loyal generals to adopt a bad plan. See, Leslie Lamport, Robert Shostak, and Marshall Pease, "The Byzantine Generals Problem" (1982) 4 ACM Transactions on Programming Languages and Systems 382.

blockchains. The latter is a more traditional way of consensus-making based on rounds of votes and is typically used in permissioned systems, where members in the network are known. Typical consensus mechanisms in blockchains are as follows:[18]

- Proof of Work (PoW): In this mechanism, a node needs to spend computational resources (solving a computational puzzle) to validate the next block. The process of solving the puzzle and creating and validating a new block is called mining, and nodes that engage in mining are called "miners."[19] Once a miner solves the puzzle and broadcasts the new block to the network, other miners verify and accept the new block.[20] There may be cases in which two or more miners solve the puzzle, and two or more different new blocks may be broadcasted in the network. In this case, a temporary fork of the chain occurs, yet the software is coded in such a way that the longer chain will be accepted by more miners and will thus survive as a legitimate chain. Proof of Work is the most popular consensus algorithm; it is used *e.g.* in Bitcoin. It is often criticised for the high amount of energy that it consumes, because solving puzzles quicker than other competitors requires many computers to do the calculations, which consumes a lot of power.
- Proof of Stake (PoS): The mechanism relies on a "stake" of the nodes in the network, typically the amount of the crypto assets held, instead of "work." In PoS, a group of validators is selected randomly from participants who hold a certain amount of stake. Validators individually attest to the block and broadcast their decision. Once a certain number of validators approve the new block, the block is appended to the chain.[21] The PoS is based on the idea that a participant who has made a substantial investment in the network and holds a substantial stake has an incentive to make the network succeed and would not work maliciously.[22]
- Delegated Proof of Stake (DPoS): This mechanism is a variation of PoS. In DPoS, validators are not selected randomly but by voting. Elected validators, called delegates or witnesses, verify and sign new blocks with their private

18 *Bashir* (n 4), 31–33.

19 ISO22739 (n 1), 3.48 and 3.49.

20 WisdomTree Market Insight (n 15), 2–3.

21 *Id.*, 3–4.

22 ITU-T Focus Group on Application of Distributed Ledger Technology (FG DLT), "Technical Report FG DLT D1.2: Distributed ledger technology overview, concepts, ecosystem" (*International Telecommunication Union*, 1 August 2019), 2 <https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d12.pdf> accessed 4 April 2023.

keys, and once the majority of the witness group approves the blocks, the blocks are appended to the chain.[23]

– Practical Byzantine Fault Tolerance (PBFT): This is the most popular Byzantine fault tolerance mechanism. In this mechanism, one of the participants becomes a leader, and the leader broadcasts a request to all nodes. The leader will wait for the responses from the nodes, and if the number of the same responses reaches equal or more than f+1 (f is the number of potential faulty nodes), the response is validated.[24] In the PBFT, all nodes must be known, so this consensus mechanism is used in permissioned systems, such as Hyperledger Fabric.

2.3 Cryptography

In blockchains, cryptographies are used to make the network secure against tampering and misuse.[25] The commonly used cryptography is "public-private key cryptography."[26] In public-private key cryptography, a pair of keys, one private and one public, is generated. The private key is a randomly generated string of numerals and letters that must be kept secret and held privately by its user. The public key is also a string of numerals and letters and freely available and published by the private key owner.[27] By using digital signature and public-private key cryptography, a message can be sent securely and anonymously. For example, A wants to send a private message to B; A encrypts the message by using A's private key and B's public key and signs the message by using A's private key. B could use A's public key to verify that the message is sent by A and has not been altered. Then B could safely decrypt the message by using B's private key and A's public key.[28]

If a holder of the digital asset wants to dispose of the asset transferred to his/her address, he/she needs to use the secret key corresponding to the address. If one forgets the private key, it is impossible to dispose of the assets corresponding to the address. Also, if the private key is stolen, all assets recorded for the address could be stolen. For example, in Japan, Coincheck, a crypto asset

23 Wisdom Tree Market Insight (n 15), 4–5.

24 Brian Curran, "What is Practical Byzantine Fault Tolerance? Complete Buginers' Guide" (*Blockonomi*, 15 August 2022) <https://blockonomi.com/practical-byzantine-fault-tolerance/> accessed 4 April 2023.

25 Bashir (n 4), 13.

26 On the public-private key cryptography, see Filippi and Wright (n 4), 14–16. ISO/TR 23576 (n 8) uses the terminologies such as "signature key" for private key and "verification key" for public key.

27 Bashir (n 4), 96.

28 Filippi and Wright (n 4), 15–16.

custodian, had ¥58 billion worth of crypto assets stolen in January 2018 after the secret key, corresponding to the addresses with which those crypto assets were recorded, was stolen.[29]

When a blockchain is used for digital assets such as Bitcoin, "wallets" are used to generate and store secret keys. The wallets can be divided into hot wallets and cold wallets depending on whether or not they are connected to the Internet. Hot wallets are online and include online wallets and mobile wallets, while cold wallets are offline and include paper wallets and hardware wallets.[30] From the viewpoint of the generation of keys, there are deterministic wallets (wallets in which multiple key pairs are derived from a single starting point called a "seed"), hierarchical deterministic wallets (a type of deterministic wallets in which child key pairs are derived from the master key pairs in a tree structure) and non-deterministic wallets (wallets in which keys are randomly generated). Also, there are multi-signature arrangements in which two or more private keys are required to make a transaction relating to an address. Considering the importance of the role of private keys in blockchains, the location of private keys could be a connecting factor. However, private keys are only string of numerals and letters and can be easily duplicated.[31] In the case of a deterministic wallet, the seed or the master key might be as important as individual secret keys. When multi-signature arrangements are used and the keys are located in different places, it would not be easy to decide which location is the most important. When a key is kept in an online or mobile wallet, there may be cases where determining its location is not easy.

There are many commercial wallet services providers that provide various types of wallet services to their customers. There are two types of wallets: custodial wallets and non-custodial wallets. In custodial wallets, the third parties (typically the wallet service providers) hold the secret keys for their customers. In non-custodial wallets, the customers hold and manage the secret keys by themselves.[32]

---

29 Yoichi Tsuchiya and Naoki Hiramoto, "How cryptocurrency is laundered: Case study of Coincheck hacking incident" (2021) 4 Forensic Science International: Reports 100241, 1–2.

30 On various types of wallets in Bitcoin, see Bashir (n 4) p 237–240.

31 Amy Held, "Does situs actually matter when ownership to bitcoin is in dispute?" (2021) 4 Journal of International Banking and Financial Law 269, 270.

32 chirag, "Custodial vs. Non-Custodial Wallets: Understanding the Difference Points" (*Appinventiv*, 3 March 2023) <https://appinventiv.com/blog/custodial-vs-non-custodial-wallets/> accessed 4 April 2023.

2.4 *Permissionless and Permissioned Blockchain*

There are two types of blockchains: permissionless and permissioned.[33] A permissionless blockchain is open to anyone, and permission or authorisation to participate in a network as a node is not required. Bitcoin and Ethereum are the most famous examples of permissionless blockchain. On the other hand, in permissioned blockchains, permission by someone who has the authority to control the access to the network (*e.g.* owner, administrator, validator) is required to participate in a network. Because of such control, in permissioned blockchain, an environment where each party on the network is known or somewhat trusted may be created.[34] Hyperledger Fabric and R3 Corda are examples of permissioned blockchains.

In a permissioned blockchain that has a person or entity who controls the access to the blockchain or manages the whole system, the location of such person or entity could be a connecting factor. For example, in the Diem project, a cryptocurrency project proposed by Facebook and originally named as the libra project, the Diem Association was set up as a body that was responsible for the Diem network.[35] In this case, the seat of the Diem Association could have been a connecting factor for some types of issues.[36]

In a permissionless blockchain, there may be a person, entity, or group of persons or entities that has a certain amount of influence over the network, even if they do not have the power to control the access, as in the case of the permissioned blockchain. For example, in relation to Bitcoin, there are developers who are contributing to the update of the Bitcoin blockchain.[37] However, they are acting on a decentralised and consensus basis, so it would be difficult to consider their location as useful connecting factors. Also, in relation to Ethereum, there is the "Ethereum Foundation," a non-profit organisation

33 World Bank Group (n 1), 11–14.

34 Filippi and Wright (n 4), 31.

35 About the Diem project, "Welcome to the Diem Project" (*Diem*) <https://www.diem.com/en-us/> accessed 4 April 2023.

36 The Diem Association applied for authorisation as a payment system in Switzerland, but in May 2021, it withdrew the application because Diem is planning to put an initial focus on the USA. See, Swiss Financial Market Supervisory Authority (FINMA), "Diem withdraws license application in Switzerland" (*FINMA*, 12 May 2021) <https://www.finma.ch/en/news/2021/05/20210512-mm-diem/>. On 31 January 2022, the Diem Association announced that it would end the Diem project.

37 Andrey Sergeenkov, "Who are Bitcoin Core's Developers?" (*Alexandria*) <https://coinmarketcap.com/alexandria/article/who-are-bitcoin-cores-developers> accessed 29 June 2023.

dedicated to supporting Ethereum, which has no power to control Ethereum.[38] Again, the location of such organisation would not be a good candidate for a connecting factor.

3 Some Use Cases

A selection of use cases and a discussion of legal disputes that may arise with respect to such use cases provide ideas as to how to think about connecting factors. Since transactions using blockchain tend to be conducted only online and in a distributed manner, it is difficult to find the location of such a transaction. As a remedy, one could refer to the location of the relevant parties or the law that they have selected expressly or impliedly. Yet the location of the parties may be difficult to determine, and they will not have always selected an applicable law. Therefore, the following discussion focuses on other possible connecting factors.

3.1 *Bitcoin*

There are two ways of holding bitcoins. One is direct holding, where aninvestor has its own Bitcoin address; the other is indirect holding, where an investor does not have its own Bitcoin address and holds Bitcoin through intermediaries that provide custody services such as crypto exchanges or wallet service providers. In the indirect holdings, an intermediary typically manages a Bitcoin address for a group of customers instead of having one Bitcoin address for each customer. Most individual investors hold indirectly. In Figure 2.2, A holds 10 bitcoins indirectly through B, a crypto exchange in the UK. Suppose C has stolen 20 bitcoins held by B, 10 of which B holds on behalf of A, and 10 of which B holds for itself. Then, C transfers 10 bitcoins to D, who does not know that the bitcoins have been stolen from B. A sues B, C, and D for the recovery of 10 bitcoins. What is the governing law? Suppose furthermore that an Italian company, E, a creditor of A and B, tries to attach the bitcoins of A and B. Which law should be applied to such claim? The answers may depend on the legal nature of the concrete claims and relevant issues. If the dispute relates to the contractual relationship between A and B, one could follow the conventional principle of party autonomy in determining the applicable law. However, for example, when A's claim is proprietary in nature, one would have

38 Ethereum Foundation, "What is the EF" (*Ethereum Foundation*) <https://ethereum.foundation/ef> accessed on 4 April 2023.

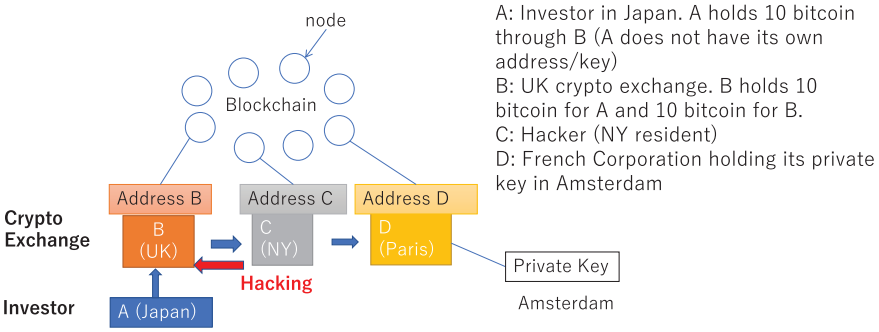

FIGURE 2.2 Diagram of bitcoin transactions

trouble identifying the situs of the object of the proprietary claim according to the *lex rei sitae* principle.

3.2 *Securities*

The blockchain may be used as a mechanism to record securities or other personal claims. Consider the example in Figure 2.3, in which Japanese investor A holds a security issued by E, an Italian company, through the intermediary B, a UK company. Instead of a book-entry in a security transfer system, the recording of E's security is made on the blockchain. A wants to sell the security to C, a New York corporation and B's customer, or give the security to C as collateral. Which law should be applied? Suppose B uses A's security as collateral for B's debt to D without A's consent and A claims the return of the security against D. Which law should determine if A or D wins? As far as the blockchain is used in the same way as the conventional recording system, one may apply the same PIL rules as used with the conventional system, in this case, the indirect book-entry security holding systems.

3.3 *Non-Fungible Tokens*

Blockchain may be used to generate and trade tokens representing an interest in physical or digital assets. The token representing the title to a unique asset is called a "Non-Fungible Token" (NFT),[39] and has been getting more and more attention. Famous examples of NFTs include a digital art object sold by

39 Clifford Chance LLP, "Non-Fungible Tokens: The Global Legal Impact" (*Clifford Chance LLP*, June 2021), 2 <https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2021/06/non-fungible-tokens-the-global-legal-impact.pdf> accessed 29 June 2023.

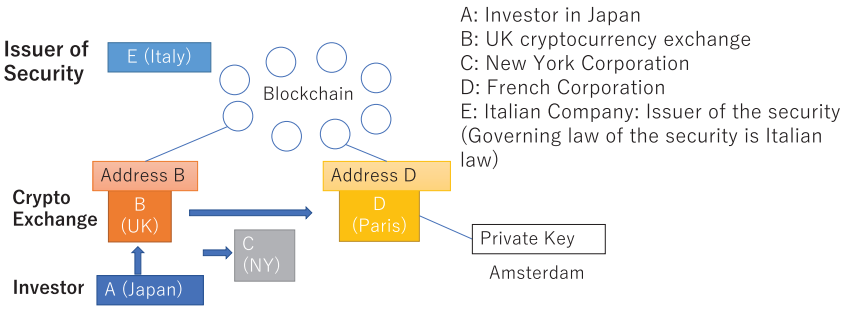

FIGURE 2.3 Diagram of securities transactions

Christie's and the video of a famous basketball player.[40] By tokenising these assets, it is expected that their tradability and liquidity would increase.[41] The legal nature of tokens and the rights that a token holder may have could differ depending on the applicable law and concrete structure of the scheme.[42]

When a token on the blockchain represents some asset, depending on the type of issues, the location of the underlying physical or digital asset and the location of the token might be considered as a connecting factor. However, determining the location of the digital asset and token would not be easy and, even if possible, could be arbitrary.

3.4 *Electronic B/L and Other Use of Blockchain Technology for Business*

There are various ongoing projects to employ blockchain technologies to replace current paper-based systems in various business areas. One of the areas in which such efforts are most advanced is the digitalisation of transportation documents or electronic "Bills of Lading" (B/L). For example, it is reported that the Mediterranean Shipping Company, one of the largest shipping companies, has adopted electronic B/L using blockchain technology.[43]

40 Caitlin Ostroff, "NFTs Explained: What's Driving Prices for LeBron James and Kings of Leon Digital Collectibles" (*Wall Street Journal*, 11 March 2021) <https://www.wsj.com/articles/nfts-explained-whats-driving-prices-for-lebron-james-and-kings-of-leon-digital-collectibles-11615205133> accessed 4 April 2023.

41 Clifford Chance LLP (n 39), 2–3.

42 A report explains that, in most of the NFT issuances relating to assets protected by copyrights, NFTs are structured so that the purchaser of an NFT owns the token itself and gets the ownership of the digital version of the underlying work, but the purchaser does not get ownership interest in or copyright to the underlying work. See *id.*, 6.

43 Mediterranean Shipping Company (MSC), "MSC Introduces New Electronic Bill of Lading for Customers Worldwide using WAVE BL's Platform" (*MSC*, 28 April 2021) <https://www

When blockchain technology is used for business, various functions must be provided and it is typical that blockchain architecture will contain several layers that provide respective function:[44]

- Network layer: the layer that implements network protocols such as P2P protocols;
- Protocol layer: the actual blockchain layer, where core consensus, transaction management, *etc.* are implemented;
- Privacy layer: the layer that provides functions to protect privacy;
- Governance layer: the layer that provides the access control mechanism;
- Integration layer: the layer that provides APIs (application programming interfaces) and a mechanism to integrate with the existing legacy, back-office and existing off-chain systems; and,
- Application layer: the layer that provides smart contracts, tools and other software to support enterprise use.

These layers work together to provide services to end users.

When a company wants to use blockchain in its business, it often aims to decentralise, improve efficiency and reduce the cost of conventional systems for record management and information processing. Rather than having individual customers participate directly in the blockchain network itself, blockchains are often used as a background technology platform to provide services to customers. As far as the blockchain simply replaces conventional computer systems or papers that were used in the back-office or as a user interface, it can be said that there is no significant difference in the relationship between the company and its customers. If so, in considering the connecting factor under PIL, it seems that the conventional way of thinking can be applied, at least with respect to the issues relating to the relationship between the company and its customers. Which law applies depends on how the system in question is structured. For example, if a system is structured such that a person who is recorded in the system managed by the company is treated as the person who is entitled to receive goods, the law applicable to the company's system (*e.g.* the

---

.msc.com/es/newsroom/press-releases/2021/april/msc-introduces-new-electronic-bill-of-lading-for-customers-worldwide-using-wave-bls-platform> accessed 4 April 2023.

44 Bashir (n 4), 660–663. There are other explanations about layer structure. For example, Livine Sanchez, "Blockchain Layers Explained: What Are They and Why Do We Need Layer Solutions?" (*CoinMarketCap*, 1 September 2021) <https://zycrypto.com/blockchain-layers-explained-what-are-they-and-why-do-we-need-layer-solutions/>, explains in 4 layers: Layer 0 (the infrastructure that supports blockchain network), Layer 1 (blockchain layer, such as Ethereum, that implements consensus mechanisms, etc.), Layer 2 (layer to solve scalability problem by taking some interactions off the blockchain), Layer 3 (application layer that serves as user interface and creates real-world use case).

law stipulated in the contract or terms and conditions for the services provided by the company) could govern various legal issues arising with respect to the system. On the other hand, if a system is structured such that a holder of the digital B/L is treated as the person that is entitled to receive goods, it would be necessary to consider the location of the digital B/L in accordance with the traditional PIL principle that the law of the location of B/L should determine the identity of the legitimate holder of the B/L.

3.5 *Smart Contracts and DAO*

One of the features of blockchain is that it can record computer programs and create an environment that computer programs recorded on a blockchain automatically perform without the involvement of humans. In such an environment, contracts executed by computer programs are called "smart contracts." A document of the International Standard Organization defines a "smart contract" as a "computer program stored in a DLT system wherein the outcome of any execution of the program is recorded on the distributed ledger."[45] Though there are various structures and levels of functions in smart contracts, in many cases, smart contracts perform what the relevant parties have agreed to and execute the commands that programmers have made to execute what the parties agreed to.[46] When a dispute arises in relation to a smart contract, could the conventional rules of PIL on contracts be applied? If so, how could the parties' express or implied choices be identified?

Smart contracts could be used among multiple parties and could create a so-called "Decentralised Autonomous Organization" (DAO). In DAOs, smart contracts define the rules of organisation and management of financial resources. Decisions on the organisation and payment of money are made based on the rules set up by smart contracts.[47]

How should one determine the law applicable to various legal issues relating to a DAO itself or the relationship created by a DAO? DAOs do not have a CEO, a head office, or staff handling daily operations, and they operate on Internet through computer codes. There is a view that DAOs could not have legal capacity, and any legal relations occurring in or with DAOs are theoretically

45 ISO22739 (n 1), 3.72.

46 Blaise Carron and Valentin Botteron, "How smart can a contract be?," in Daniel Kraus, Thierry Obrist, and Olivier Hari (eds), *Blockchains, Smart Contracts, Decentralised Autonomous Organizations and the Law* (Edward Elgar 2019), 101, 108.

47 Ethereum, "Decentralized Autonomous Organizations (DAOs)" (*Ethereum*) <https://ethereum.org/en/dao/> accessed 29 June 2023.

considered as relations between the end-users of the DAO.[48] If there is no legal capacity under the applicable law, it would be an option to consider a governing law that would be applied to the relationship between the end-users. However, which law should be applied to determine the legal capacity of an organisation that exists virtually and is operated by computer programs? If a DAO relates to a project that has a close connection to a location in the real world, that location could be a connecting factor, but such a case would be rare.

4 Conclusion

This chapter reviewed the technical features of blockchain and examined possible connecting factors in some typical use cases. As discussed in this chapter, the blockchain itself and use cases of blockchain raise a variety of difficult PIL questions. These difficulties include not only whether existing rules of PIL relating to contracts, tort, property rights, corporations, *etc.* could be applied to transactions using this new technology, but also, even if the existing rules may be applied, how to identify connecting factors using the conventional rules, such as location, place of performance, choice of parties, *etc*. In addition, the scope of legal issues governed by the applicable law could raise difficult questions.[49]

On the other hand, it is also important to note that laws must be technology-neutral. It is not appropriate for the applicable rules are different depending on non-essential technical differences.

In order to make a balanced decision, it is important to have a good understanding of blockchain technology and the reality of its use cases.

---

48 Kryszof Wojdyto, "What is DAO from the legal perspective?" (*Coalition for Polish Innovations*) <https://www.wyoleg.gov/InterimCommittee/2019/S3-20190506DAOLegalPerspectives.pdf> accessed 29 June 2023.

49 For example, in the drafting process of The Hague Convention on the Law Applicable to Certain Rights in Respect of Securities held with an Intermediary, there was a debate about the scope of the issues governed by the applicable law. Convention of 5 July 2006 on the Law Applicable to Certain Rights in Respect of Securities held with an Intermediary, full text available at <https://assets.hcch.net/docs/3afb8418-7eb7-4a0c-af85-c4f35995bb8a.pdf> accessed 30 May 2022.

CHAPTER 3

Should Crypto-Asset Regulation Be Technology-Neutral?

Bruno Mathis

1 Introduction

Almost every legislative project or public consultation on crypto assets that comes out in the world defends the principle of technological neutrality. Where does this principle come from? How is it applied when crypto-asset regulation is drafted?

On the face of it, the question of whether crypto-assets regulation should be technology-neutral appears to be an oxymoron: crypto assets are technology-specific. But it is no more so than "Should ICT Regulation be Technology-Neutral," as Professor Koops wondered.[1] Technological neutrality of regulation is not a novel issue: the theme dates back to the advent of the Internet.[2] It developed with the legal issues of electronic communications[3] and property rights over digital works.[4] In the financial sector, the concept was restricted to the meaning of interoperability rules aimed at levelling the playing field.[5]

1 Bert-Jaap Koops, "Should ICT Regulation be Technology-Neutral," in Bert-Jaap Koops et al. (eds), *Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-liners* (The Hague: TMC Asser 2006), 77–108.

2 See Chris Reed, "Taking Sides on Technology Neutrality" (2007) 4 Script-ed 264.

3 See for instance Ian Hosein and Alberto Escudero, "Understanding Traffic Data and Deconstructing Technology-neutral Regulations" (*CiteSeerX*, 7 March 2002) <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.475.5291&rep=rep1&type=pdf>.

4 See Dan L. Burk and Mark A. Lemley, "Is patent law technology-specific?" (2002) 17 Berkeley Technology Law Journal 1157, 1157–1208.

5 See Paola Lucantoni, "Strumenti digitali e finanza," in Fabrizio Maimeri and Marco Mancini (eds), *Quaderni di Ricerca Giuridica: della Consulenza Legale, Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale* (Banca d'Italia 2019), vol. 87, 291–310.

© BRUNO MATHIS, 2023 | DOI:10.1163/9789004514850_005
This is an open access chapter distributed under the terms of the CC BY-NC-ND 4.0 license.

The issue is important because crypto assets,[6] and the technology that allows them to circulate, are difficult to apprehend and their legal qualification is thorny. First, it took a crypto asset, Bitcoin,[7] born in 2008, to somehow reveal the potential of the blockchain, its underlying technology, from 2014. Bitcoin was emulated, inspiring alternative coins (altcoin), and then other crypto assets emerged, performing equivalent functions without necessarily using blockchains. Today, the term "crypto asset" is commonly defined as a cryptographically secured digital representation of value of contractual rights that uses some type of blockchain and can be transferred, stored or traded electronically. The blockchain challenged again the principle of technological neutrality of law, while some defended, on the contrary, a *lex cryptographia,*[8] or that law should at least treat the blockchain as an "infrastructural commons."[9]

The following vogue for stablecoins and security tokens questioned how financial law in particular could be neutral to these instruments. Because the term of blockchain is technical and looks narrow, the expression of Distributed Ledger Technology (DLT) appeared in 2016 and has gradually established itself since then.[10]

It is as difficult to identify the common properties of crypto assets as their distinctive properties with existing legal objects. Lawmakers rightfully fear the opening of Pandora's box in positive law. Still, over the last three years, legislative and regulatory initiatives have been multiplying with respect to crypto assets all over the world. The vast majority of these initiatives set technological neutrality as their objective, however fuzzy the concept.

This chapter is structured as follows. Section 2 describes and analyses the limits of the three arguments that lie at the heart of this principle – future-proofing, impartiality and functional equivalence –, then considers other hidden motivations. Section 3 discusses the implications of that principle in the writing of legal definitions and rules, and for Private International Law (PIL).

---

6 For more details, see Fabian Schär and Aleksander Berentsen, *Bitcoin, Blockchain, and Crypto-assets: A Comprehensive Introduction* (MIT Press 2020).

7 Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (*Bitcoin*, 31 October 2008) <https://bitcoin.org/bitcoin.pdf>.

8 Aaron Wright and Primavera de Filippi, "Decentralized Blockchain Technology and the Rise of Lex Cryptographia" (*SSRN*, 25 July 2017) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664>.

9 Georgios Dimitropoulos, "The Law of Blockchain", 95 Washington Law Review 1117 (2020).

10 Mark Walport, "Distributed ledger technology: beyond blockchain" (*UK Government Office for Science*, 19 January 2016) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf>.

2 The Case for Technology-Neutrality

The technology-neutrality principle is based on three arguments, which are not mutually exclusive.

2.1 *Future-proofing*

The future-proofing argument seeks to protect against the risk of change or obsolescence. Under this criterion, common law would be intrinsically neutral to technology if, as the UK Jurisdiction Taskforce maintains, "English law, as a well-developed flexible common law system, [...] is well able to adapt to deal with fast-changing technologies."[11]

According to the Landau Report, which served as a doctrinal basis for the introduction of crypto assets in French law, "imposing standards to players and technology today would paralyze progress."[12] These would be technology-specific and therefore premature. On the contrary, provisions capable of standing innovations over time would bring legal certainty. The concern is shared by the Permanent Bureau of the Hague Conference on Private International Law (HCCH)[13] and UNIDROIT,[14] which both seek to develop future-proof principles in their respective areas.

On one occasion, German regulator BaFin implied that its national law was already future-proof. The regulator had sanctioned an individual for trading Bitcoin on the ground Bitcoin was a unit of account (*Rechnungseinheit*) within the meaning of a law adopted 10 years before. Its reasoning was that the unit of account was legally defined as a financial instrument, and because the trader did not have the corresponding banking licence, he operated illegally. But a

11 UK Jurisdiction Taskforce of the LawTech Delivery Panel, "Public consultation - The status of crypto-assets, distributed ledger technology and smart contracts under English private law" (*The LawTech Delivery Panel*, May 2019) <https://www.enyolaw.com/downloads/ukjt-consultation-cryptoassets-smart-contracts-may-2019%20(1).pdf> accessed 31 May 2022.

12 Jean-Pierre Landau & Alban Genais, «Les crypto-monnaies - Rapport au Ministre de l'Économie et des Finances» (4 July 2018), 45 <https://www.economie.gouv.fr/files/files/2019/Rapport_LandauVF.pdf?v=1570634503>.

13 Hague Conference on Private International Law, "Developments with respect to PIL implications of the digital economy, including DLT" (*HCCH*, 4 November 2020, §2 <https://assets.hcch.net/docs/8bdc7071-c324-4660-96bc-86efba6214f2.pdf>.

14 International Institute for the Unification of Private Law, "Digital Assets and Private Law Working Group: First Session (remote), Rome, 17–19 November 2020" (*UNIDROIT*, March 2021), §32 <https://www.unidroit.org/english/documents/2021/study82/wg01/s-82-wg01-04-e.pdf> accessed 31 May 2022.

court of appeal contested that interpretation because "the wording of the law is not open to an interpretation according to which bitcoins that only appeared after the enactment of the law could be subsumed under the concept of a unit of account."[15] Future-proofing is not writing a blank cheque on the future. It cannot be presumed beyond what the legislator can reasonably imagine at the time of drafting the law.

In 2009, the European Union adopted its second directive on electronic money,[16] which stated that the definition of electronic money "should be wide enough to avoid hampering technological innovation and to cover not only all the electronic money products available today in the market but also those products which could be developed in the future."[17] Some crypto players then applied for a licence to operate as an electronic money institution to issue payment tokens backed by a reserve of *fiat* money. Yet, in 2020, the European Commission preferred to introduce the "e-money token," for that purpose, in its proposal of a regulation on markets in crypto assets (MiCA).[18] A broad, future-proof, definition does not guarantee that pressure will not build over time to bring greater legal certainty to a specific technology.

2.2 *Impartiality*

The argument of impartiality is to protect against the risk of discrimination between economic actors with respect to their technical choices. As the saying goes, "regulation should not pick winners and losers." For the Financial Action Task Force (FATF), the global money laundering and terrorist financing watchdog, "the requirements applicable to virtual assets, as value or funds, to covered [virtual assets] activities, and to [virtual assets services providers] apply irrespective of the technological platform involved."[19] For the EU Commission, "Union financial service legislation should not favour a particular technology."[20]

---

15 Kammergericht Berlin (4. Strafsenat) (KG Berlin), *Urteil vom 25.9.2018* – (4) 161 Ss 28/18 (35/18) (ECLI:DE:KG:2018:0925.4.35.18.00). (Criminality of trading bitcoins).

16 Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC, [2009] OJ L267/7.

17 *Id.*, Recital 8.

18 Proposal for a Regulation of The European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, [2020] COM/2020/593 final ("MiCA").

19 Financial Action Task Force, "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers" (*FATF*, 21 June 2019), 9 <https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf>.

20 MiCA (n 17), Recital 6.

The principle applies to consensus mechanisms, protocols, smart contracts and platforms (Ethereum, Tezos, Ripple, etc.). To start with, it should be indifferent whether the platform has chosen or not a blocks-based architecture. Likewise, there should be no discrimination against crypto players based on whether their distributed ledger is public (or permissionless), rather than private (or permissioned), as long as they meet their security or know-your-customer (KYC) obligations by other means.

Impartiality is not just a question of competition between crypto players. The German government puts DLT on the same level as conventional technologies. According to its preliminary report on the regulatory treatment of electronic securities and crypto tokens, "rules on electronic securities will be technologically neutral, *i.e.* the use of blockchain technology will not be privileged in any way, especially in view of the high current energy needs of public blockchain technologies and their negative effects on the climate."[21] As for the UK Treasury, it stresses that what it calls "stable tokens" could be designed using other types of technology than DLT, and require a crypto asset classification that is technology-"agnostic."[22]

2.3 *Functional Equivalence*

The argument of functional equivalence refers to the adage "same business, same risks, same rules" or to the principle of "substance over form," that underlies US federal law. According to this idea, it would neither be appropriate to legislate on Bitcoin alone, if the same concepts apply to alternative coins (*altcoins*), nor on security tokens if they have the same function as book-entry securities.

The principle of functional equivalence applies more easily to the category of investment tokens, in which the token can be seen as a vehicle for the alternative booking of the security in the account. It is implicit in the commentary on the Luxembourg bill opening up the circulation of securities to the blockchain, according to which "these new methods of managing securities

21 Bundesministerium der Finanzen, "Key-issues paper on the regulatory treatment of electronic securities and crypto tokens – Allowing for digital innovation, ensuring investor protection" (Bundesministerium der Finanzen, 7 March 2019), 2 <https://www.bundesfinanzministerium.de/Content/EN/Downloads/Financial-Markets/2019-03-25-electronic-securities-and-crypto-tokens-key-issues-paper.pdf?__blob=publicationFile&v=4>.

22 HM Treasury, "UK regulatory approach to crypto-assets and stablecoins: Consultation and call for evidence" (*HM Treasury*, 7 January 2021), 6 <https://www.gov.uk/government/consultations/uk-regulatory-approach-to-cryptoassets-and-stablecoins-consultation-and-call-for-evidence>.

accounts constitute alternatives to the methods of dematerialisation that practice and the law already know."[23] The OECD also draws this parallel, noting that "Tokenisation can be seen as merely replacing one digital technology (electronic book-entries in securities registries of central securities depositories) with another (cryptography-enabled dematerialised securities based on DLT-enabled networks), therefore raising no issues in jurisdictions with a technology-neutral approach to regulation."[24] One author sees legacy information systems or centralised-ledger technology (CLT), as an alternative architecture to DLT.[25]

Functional equivalence can be assessed at the level of each processing step. The European Central Bank stated that "the same technology-neutral rules and legal provisions shall therefore apply, to the extent possible, to the issuance, bookkeeping and use of these tokens as they apply to the financial assets they represent."[26] It also applies to support functions. The French Treasury pointed out that for many players, the law applicable to data management, security and interoperability requirements, or even customer knowledge (KYC), do not seem to need to be specified in the law and should not therefore be specifically defined with regard to the blockchain.[27]

However, applying a functional equivalence principle to security tokens is tricky, as the European Commission half-recognises: "although existing EU *acquis* regulating trading and post-trading activities strives to be technologically neutral, existing regulation reflects a conceptualisation of how financial markets currently operate, clearly separating the trading and post-trading

23 Fernand Etgen, «Projet de loi portant modification de la loi modifiée du 1er août 2001 concernant la circulation de titres» (*Le Gouvernement du Grand-Duché de Luxembourg*, 28 September 2018), Doc. No. 7363 <https://data.legilux.public.lu/file2/2019-10-14/800>.

24 Organisation for Economic Co-operation and Development (OECD), "The Tokenisation of Assets and Potential Implications for Financial Markets" (*The OECD Blockchain Policy Series* 2020), 8 <https://www.oecd.org/finance/The-Tokenisation-of-Assets-and-Potential-Implications-for-Financial-Markets.pdf> accessed 31 May 2022.

25 Alain Rocher, "Réglementation & blockchain : le défi de la neutralité technologique" (2020) *Revue Banque* No. 849.

26 ECB Crypto-Assets Task Force, "Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures (Occasional Paper Series No. 223)" (*European Central Bank*, 14 May 2019), 9 <https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op223~3ce14e986c.en.pdf>.

27 DG Trésor, "Synthèse de la consultation publique sur la transmission de certains titres financiers au moyen de la technologie «blockchain» (*Ministère de l'Économie*, 31 August 2017) <https://www.tresor.economie.gouv.fr/Articles/2017/08/31/synthese-de-la-consultation-publique-sur-la-transmission-de-certains-titres-financiers-au-moyen-de-la-technologie-blockchain>.

phase of a trade life cycle."[28] Thus, even if it "strives" to, European financial regulation may not be so technologically neutral in retrospect. More specifically, seeking functional equivalence for security tokens implies that the long-standing postulate of a necessary functional split between trade execution and trade settlement is still valid for these securities. One respondent to the Swiss consultation on the subject put it more bluntly: that the national Financial Market Infrastructures Act "is in no way technology neutral […] and the structure with trading venues, CCPs and CSDs is not God-given, but the result of technologies available so far."[29]

2.4 *Hidden Motivations*

The argument of technological neutrality is occasionally used as a pretext. On the one hand, it helps to dodge politically sensitive issues, in particular that of Bitcoin, which no legal text calls by name. As it represents 65% of the capitalisation of cryptocurrencies,[30] a specific legal recognition could have been considered for it. But this would have led to strong opposition from central bankers.[31] Conversely, central bankers made theirs the expression of "central bank digital currency," where the word "digital" was conveniently preferred to "crypto," in a particularly accomplished form of technological neutrality. It allows them to look good after having been very critical of cryptocurrencies, and to have full leeway in their own technological choices.

On the other hand, the argument helps to hide the possible embarrassment of the legislator caused by the technicality of the subject. Opting for wordings as least technical as possible helps the writer to stay in his comfort zone

28 European Commission, "Public consultation an EU framework for markets in crypto-assets" (*Better Finance*, 19 March 2020), 97 <https://betterfinance.eu/wp-content/uploads/Better-Finance-formal-response-markets-in-crypto-assets.pdf>.

29 Wenger & Vieli, „Stellungnahme zur Vernehmlassung betreffend Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen verteilter elektronischer Register" (*Wenger & Vieli*, 27 June 2019), 560/589 on <https://www.fedlex.admin.ch/filestore/fedlex.data.admin.ch/eli/dl/proj/6019/15/cons_1/doc_5/de/pdf-a/fedlex-data-admin-ch-eli-dl-proj-6019-15-cons_1-doc_5-de-pdf-a.pdf>.

30 CoinMarketCap, "Today's Cryptocurrency Prices by Market Cap" (*CoinMarketCap*) <https://coinmarketcap.com> accessed 29 June 2023.

31 As evidenced by the qualification of Bitcoin as the "evil spawn of the financial crisis" by a member of the executive board of the ECB, in November 2018. Claire Jones, "ECB official dubs bitcoin 'evil spawn of the financial crisis'" (*Financial Times*, 15 November 2018) <https://www.ft.com/content/92c4737e-e8ed-11e8-885c-e64da4c0f981>.

and avoid public challenge. Professor Gautrais sees the quest for technology-neutrality as a "salvationist martingale"[32] to apprehend technological change.

Market regulators are also tempted to dodge the issue. The (British) Financial Conduct Authority (FCA) explains that "historically, the FCA's philosophy has been one of 'technology neutrality' *i.e.* not to regulate specific technology types, only the activities they facilitate and the firms carrying out these activities." That claim allows it to hide that - like any other regulator - it has not built up sufficient technical expertise to provide guidance, specifically on the difficult question of the monitoring of on-chain transactions for anti-money laundering purposes. The Agency for Digital Italy (AGID), for its part, referring to smart contracts rather than specifically to crypto assets, suggests a "particular caution in relation to indications or options that could compromise the necessary neutrality technology of the rules to be adopted."[33] The parliament had imprudently introduced the smart contract into national contract law[34] and given the Agency three months to provide guidelines.[35] The requirement of technological neutrality is used as a dubious but convenient explanation to avoid putting the blame on an overly ambitious legal provision.

3 Implications for Legislation

3.1 *Naming Legal Objects*

The appearance in 2016 of the term "distributed ledger technology" already marks the concern to define it as generically as possible. Indeed, the intrinsic benefits of blockchain, unforgeability and the absence of double-spending risks, can be obtained without transactions necessarily being recorded in the form of chains of blocks. However, DLT remains a technical term. It does not provide information on its function. The epithet "distributed" has been chosen to refer to the identical replication of a transaction on multiple computers, or "nodes," to prevent any subsequent fraudulent alteration. However, it is difficult to apply to the Lightning Network, a variant of a blockchain that organises communication between only two nodes for the benefit of increased

32 Vincent Gautrais, *Neutralité technologique : rédaction et interprétation des lois* (Montréal: Éditions Thémis 2012), 268.

33 Mila Fiordalisi, "Blockchain, che fine hanno fatto le linee guida Agid?" (*Corriere Communicazioni*, 18 June 2020) <https://www.corrierecomunicazioni.it/digital-economy/blockchain-che-fine-hanno-fatto-le-linee-guida-agid/>.

34 Decree-Law No. 135 of December 14, 2018 ratified by law of 19 February 2019, Urgent Provisions on Supporting and Simplifying Companies and Public Administration (D.L. No. 135), Gazzetta Ufficiale (G.U.), Dec. 14, 2018, art. 8 ter. al. 2 <https://www.gazzettaufficiale.it/eli/id/2019/02/12/19A00934/sg>.

35 *Id.*, al. 4.

performance. In any case, for want of a better definition, it will be the one retained by the European supervisory agencies in their simultaneous advice of 9 January 2019, and subsequently adopted by the Swiss Federal Council and the European Commission for their respective legislative projects.

Refining the definition of DLT remains hard, and may betray a lack of understanding of the technology. For instance, the EU Commission defines it as "a class of technologies which support the distributed recording of encrypted data."[36] This is wrong. Though underlying data are secured by cryptographic means, recorded data are usually not encrypted.

The search for lowest common denominators leads to fuzzy definitions. For example, many information systems could be qualified as "shared electronic recording devices" (*dispositifs d'enregistrements électroniques partagés*), within the meaning of the French blockchain ordinance, without having anything to do with the blockchain. So-called "simple" uncertificated securities, in Switzerland, are no less registered than so-called "registered" uncertificated securities,[37] and, in Japan, what the law now calls "electronically recorded transferable rights" appears to be a description of existing dematerialised securities.[38] If the crypto asset, within the meaning of MiCA, is a "digital representation of value or rights which may be transferred and stored electronically, using distributed ledger or similar technology,"[39] why couldn't a traditional database qualify as a "similar technology" for that purpose?

The Principality of Liechtenstein is the jurisdiction that went furthest in its effort of conceptualisation. Its government noted that "the terms 'virtual' or 'crypto' describe a technological form and, for reasons of technological neutrality, are not appropriate to be used as an umbrella term in the context of

36 Proposal for a Regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology, [2020] COM/2020/594 final, art. 2(1).

37 New arts. 973c and 973d of the Swiss Code of Obligations (Federal Act on the Amendment of the Swiss Civil Code (Part Five: The Code of Obligations) of 30 March 1911, SR 220), resulting from the Loi fédérale sur l'adaptation du droit fédéral aux développements de la technologie des registres électroniques distribués du 25 septembre 2020, FF 2020 7559.

38 Sygna, "Japan's Financial Services Agency (FSA) To Enforce New Crypto-Asset Exchange Regulations from 1 May 2020" (*Sygna*) <https://www.sygna.io/blog/japan-crypto-asset-regulation-financial-services-agency-changes-psa-fiea-may-2020/> accessed 29 June 2023.

39 MiCA (n 17), art. 3(1)(2).

this Law."[40] The government preferred to define "trustworthy technologies."[41] Here again, the definition is questionable, for three reasons. Trust, or rather, confidence, is indescribable and cannot be decreed. It cannot be reduced to the unforgeability guaranteed by immutability, which itself depends on the consensus mechanism used. And generally speaking, the security of uses will depend less on technology than on the applications based on it.

The principle of technology neutrality also leads lawmakers to refrain from naming objects that are technology-specific. None of the legislative initiatives on crypto assets so far mentions the wallet or the blockchain address, for instance. To avoid naming it, the French lawmaker used a circumlocution: "registration in a shared electronic registration device serves as account registration,"[42] which leaves open a registration to *any* wallet in that shared electronic registration device.

Likewise, the private key is seldom mentioned, though its role is essential. This key, which could be stored on a hardware device (cold storage) or by software means (hot storage), gives access to crypto assets. It can be duplicated, giving equal access to more than one person, or cut up between multiple signatories, thereby defining who might have effective and exclusive control of underlying assets – or not. Governance of private keys does have effects in ownership and bankruptcy law.

3.2 *Designing Technology-Neutral Rules*

The technology-neutrality principle leads legislators and regulators to write as few rules as possible. The Chairman of the US Securities and Exchange Commission once epitomised his stance by saying: "I'm not going to change rules just to fit a technology."[43] Other policy-makers seek minimal wordings. The French government managed few amendments to its national

---

40 Government of Liechtenstein, "Report and Application of the Government to the Parliament of the Principality of Liechtenstein Concerning the Creation of a Law on Tokens and TT Service Providers (Tokens and TT Service Provider Act; TVTG) and the Amendment of Other Laws (No. 54/2019)" (*Impuls Liechtenstein*, 7 May 2019), 12 <https://impuls-liechtenstein.li/wp-content/uploads/2021/02/Report-and-Application-TVTG-extract.pdf>.

41 Law of 3 October 2019 on Tokens and TT Service Providers (Token and TT Service Provider Act; TVTG), art. 2(1)(a): "Trustworthy Technology (TT): Technologies through which the integrity of Tokens, the clear assignment of Tokens to TT Identifiers and the disposal over Tokens is ensured."

42 French Monetary Code, art. L211-3: "L'inscription dans un dispositif d'enregistrement électronique partagé tient lieu d'inscription en compte."

43 Tim Fries, "SEC Chairman Jay Clayton: 'I'm not going to change rules just to fit a technology'" (*The Tokenist*, 15 September 2019) <https://tokenist.com/sec-chairman-jay-clayton-im-not-going-to-change-rules-just-to-fit-a-technology/>.

law. Its "blockchain ordinance"[44] essentially equated the distributed ledger to a securities account in a couple of legislative provisions.

Some rules may look tautological or abstruse. For example, the EU-proposed pilot regime imposes that "the number of DLT transferable securities recorded on the DLT MTF equals the total number of such DLT transferable securities in circulation on the digital ledger technology at any given time."[45] That particular rule actually means that in case the MTF manages customer individual attributions off-chain while storing aggregated crypto assets on a single omnibus wallet on-chain, then it must check that the sum of the former equals the latter. The obscure wording is here again due to a reluctance to define the wallet by its name.

The Swiss Federal Council felt that the technology-neutrality principle had its limits. To them, the introduction of a new DLT-specific market infrastructure constitutes "an appropriate derogation from the principle of technological neutrality. Such a technology-specific approach also has the added merit of leaving the regulation of existing capital market infrastructures unchanged."[46] The European Banking Authority's FinTech Knowledge Hub wants "to foster technological neutrality in regulatory and supervisory approaches on an ongoing basis."[47] The implementation of the technology-neutrality principle thus reveals a cognitive bias: if the legacy legal framework is used as the basis for amendments, the new legal framework is rather skewed toward legacy technologies than actually neutral.

Applied literally, the technology-neutrality principle would leave some issues unaddressed. By this standard, Bitcoin, which is technology specific and has no functional equivalent, would remain unregulated. It would be difficult to punish ill-conduct on an unnamed object, like, for instance, urging Europe to fight against laundering through Bitcoin[48] while MiCA makes a point of not mentioning Bitcoin in its taxonomy of crypto assets. Not a word would describe

---

44 Ordonnance No. 2017–1674 du 8 décembre 2017 relative à l'utilisation d'un dispositif d'enregistrement électronique partagé pour la représentation et la transmission de titres financiers.

45 [2020] COM/2020/594 final (n 35), art. 4(2)(b).

46 Swiss Federal Council, «*Message relatif à la loi fédérale sur l'adaptation du droit fédéral aux développements de la technologie des registres électroniques distribués* (FF 2020 223)» (*Swiss Federal Council*, 27 November 2019), 40 <https://www.fedlex.admin.ch/eli/fga/2020/16/fr>.

47 European Banking Authority, "FinTech Knowledge Hub" (*EBA*) <https://eba.europa.eu/financial-innovation-and-fintech/fintech-knowledge-hub> accessed 7 November 2020.

48 Reuters Staff, "ECB's Lagarde calls for regulating Bitcoin's 'funny business'" (*Reuters*, 13 January 2021) <https://www.reuters.com/article/us-crypto-currency-ecb-idUSKBN29I1B1>.

how to safekeep private keys. Suitability and appropriateness tests protecting investors would not be modified to address technology-specific risks. Investors would be recognised no rights over tokens created by a 'fork', a DLT-specific function. Simultaneous securities delivery against settlement would apply in whatever configuration, specifically *fiat* currency against security tokens, or payment tokens against book-entry securities. Refraining from drafting technology-specific provisions to deal with new operational risks may thus come at the expense of the requirements of financial security and investor protection.[49]

Too much neutrality in regulation will confer as much discretionary power on supervisors or judges. As Professor Koops had concluded, "regulation should be as much technology-neutral as is compatible with sufficient legal certainty."[50]

Another risk is to forfeit DLT-specific benefits and jeopardise the profitability of investing in DLT. There would be no self-custody of security tokens as this does not exist for book-entry securities. They would be traded over trading venues born from a previous technology era and their transactions recorded by a central securities depository. Multiple interfaces between legacy and DLT-based technologies would have to be developed, for every single processing step, and raise as many interoperability issues. A large part of additional developments would have to be conducted off-chain, and investment firms, sole eligible operators, may not see a return on such an investment. Law may be indifferent to technology, but economics of DLT is not indifferent to law. If, to comply with law, DLT should cost the same as conventional IT, why invest in it?

3.3 *Implications for PIL*

The technology-neutrality principle already has its limits on PIL. In the EU, a person domiciled in a Member State may be sued in another Member State, among other cases, "in matters relating to tort, delict or quasi-delict, in the courts for the place where the harmful event occurred or may occur."[51] In some defamation cases, CJEU jurisprudence suggests that technology determines the place where a harmful event may occur: for a print publication,

49 See Bruno Mathis, "Régulation des crypto-actifs : la Suisse vise la neutralité technologique" (*HAL ESSEC*, 5 November 2020) <https://hal-essec.archives-ouvertes.fr/hal-02991122/document>.

50 Koops (n 1).

51 Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, [2012] OJ L351/1, art. 7(2) ("Brussels I bis").

where this publication is distributed,[52] for an online one, where the victim has its centre of interests, generally its domicile.[53] Assessing connecting factors will be no easier for crypto assets, which are ubiquitous in nature. Where does harm occur when a flaw in a smart contract results in denied, or corrupt, transactions, or when a so-called oracle feeds that smart contract with fake data? While deducing the competent jurisdiction(s) from a breakdown of financial or social damages on a territorial basis may be feasible for online-publishing cases, it might be not for crypto-asset-related ones.

Should a country decide to liken the crypto asset to a tangible, as Germany recently did,[54] this does not make it easier to locate it, and comply with the traditional *lex rei sitae* principle. Security tokens are akin to securities, so their conflict-of-laws rules could be adapted from those applying to traditional securities. However most other crypto assets, especially Bitcoin and utility tokens, have no functional equivalents in the real world, so that principle is useless for them in the setting of *ad hoc* conflict-of-laws rules.

The UK's Financial Markets Law Committee (FMLC) was first to propose new connecting factors to determine the applicable law, such as the location of any original coder, operator or holder of the private key.[55] These factors are influenced by the underlying technology, especially the last one, which at least implies the use of an encryption mechanism. These are technology-driven, not technology-neutral proposals. Anyway, the wide variety of operational models makes it difficult to identify and prioritise connecting factors. In the case of an "exogenous" crypto asset, which has a connection with an asset outside the DLT, there might be too many factors to choose from. In the case of a Decentralised Autonomous Organisation (DAO), where any coder, operator or participant is anonymous by design, there might be none at all. The writing

52 Judgment of the Court of 7 March 1995, *Fiona Shevill, Ixora Trading Inc., Chequepoint SARL and Chequepoint International Ltd v Presse Alliance SA.*, Case C-68/93 (ECLI:EU:C:1995:61) ("*Shevill*").

53 Judgment of the Court (Grand Chamber) of 25 October 2011, *eDate Advertising GmbH and Others v X and Société MGN LIMITED*, Joined Cases C-509/09 and C-161/10 (ECLI:EU:C:2011:685); Judgment of the Court (Grand Chamber) of 17 October 2017, *Bolagsupplysningen OÜ and Ingrid Ilsjan v Svensk Handel AB*, Case C-194/16 (ECLI:EU:C:2017:766).

54 Gesetz zur Einführung von elektronischen Wertpapieren vom 3. Juni 2021 (BGBL. I S. 1423), art. 1 §2(3). See also Bruno Mathis, «Les crypto-actifs en droit allemand : plus de questions que de réponses» (*Wolters Kluwer*, 2 March 2020) <https://www.actualitesdudroit.fr/browse/tech-droit/blockchain/26194/les-crypto-actifs-en-droit-allemand-plus-de-questions-que-de-reponses>.

55 Financial Markets Law Committee, "Distributed Ledger Technology and Governing Law: Issues of Legal Uncertainty" (*FMLC*, March 2018), §6.16 to §6.24 <http://fmlc.org/wp-content/uploads/2018/05/dlt_paper.pdf> accessed 31 May 2022.

of applicable law rules that tackle such diverse situations will therefore prove inevitably driven by technology. To start with, no rule could provide that the applicable law is that of a party whose location cannot be identified as a result of technology.

In an amended version of the proposal of a regulation on the law applicable to the third-party effects of assignments of claims,[56] the Council of the EU proposes to cover "claims arising from assets irrespective of the technology used for their issuance, transfer or storage, thus including claims arising out of crypto assets that are not financial instruments."[57] This wording recognises the functional equivalence of electronic money as per Directive 2009/110/EC and e-money tokens as per MiCA, and is consistent with the future technology-neutral definition of the financial instrument, as set out by the proposed digital finance package.[58] The law applicable to the assigned claim would govern the third-party effects of the assignment of claims arising out of crypto assets.[59] However, the proposed regulation does not say what law would apply when the assigned claim not only arises out of a crypto asset, but is itself recorded on the DLT, linking anonymous participants,[60] that is, when the law of the assigned claim cannot be determined. It also excludes the assignment of claims represented by a book-entry,[61] a term that reveals some technology legacy rather than technology neutrality. Applying the principle of technological neutrality in the drafting of every single legislative provision therefore seems as tricky for crypto assets as it is for other topics of PIL like defamation.

4 Conclusion

As noted in the introduction, it is striking to note that the question of technological neutrality is raised in countries which have started to legislate or,

56 Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on the law applicable to the third-party effects of assignments of claims, [2021] 2018/0044(COD), 9050/21.

57 *Id.*, § 16.

58 Proposal for a Directive of the European Parliament and of the Council amending Directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341, [2020] COM/2020/596 final, art. 6(1) adds to the definition of the financial instrument "including such instruments issued by means of distributed ledger technology."

59 Council of the European Union (n 54), art. 4(2).

60 A crypto-asset may be lent, or pledged, on the DLT, its refund being executed by a smart contract when the loan expires.

61 *Id.*, art. 1(2)(g).

plans to legislate on crypto assets. But the intangible and ubiquitous nature of crypto assets is inescapable, and calls for adequate, technology-specific, responses in both public and private law.

Alternatively, all the jurisdictions adopting instruments dedicated to crypto assets would logically converge toward similar provisions. Technology-specific regulation should ease harmonisation of national laws and increase legal certainty of cross-border crypto-asset transactions. But harmonisation is not what is happening.[62]

In theory, it is possible to enact technologically neutral laws within each country, or internationally harmonised crypto-asset specific laws, but less easy to achieve technological neutrality and international harmonisation at the same time. And in practice, neither one is likely.

---

62 Matthias Lehmann, "National Blockchain Laws as a Threat to Capital Markets Integration", 26, Uniform Law Review, 148.

CHAPTER 4

Is Bitcoin out of Reach for Private International Law?

David Sindres

1 Introduction

Bitcoin was launched in 2008 and appears as the first application of the blockchain technology. It remains, to date, the best known and the most used cryptocurrency.[1] Like other cryptocurrencies, Bitcoin aims to become an alternative to State and multistate currencies, such as the Euro. The importance it has gained in practice over the past few years has grasped the attention of legal scholars, who tend to perceive Bitcoin as a challenge to traditional legal rules and therefore reflect upon the ways the latter can be applied to this technological new deal.

Although these reflections concern, first and foremost, rules of substantive law, such as contract law, they also extend to Private International Law (PIL).[2]

1 See in this regard, Mathias Audit, "Le droit international privé confronté à la blockchain" (2020) 4 Revue critique de droit international privé, 669–682. According to a French study published in 2018, the bitcoin accounts for 0,2 % of the volume of financial transactions within the Eurozone (see Jean-Pierre Landau and Alban Genais, "Les crypto-monnaies, Rapport au Ministre de l'Economie et des Finances" (*Ministry of Economy and Finance*, 4 July 2018), 3 <https://www.vie-publique.fr/rapport/37499-les-crypto-monnaies> accessed 29 June 2023).

2 See esp. Matthias Lehmann, "Who owns Bitcoin ? Private Law facing the Blockchain" (2019) European Banking Institute Working Paper Series 2019, 42; Giesela Rühl, "Smart (Legal) Contracts, or: Which (Contract) Law for Smart Contracts," in Benedetta Cappiello and Gherado Carullo (eds), *Blockchain, Law and Governance* (Springer 2021), 159 et seq.; Florence Guillaume, "Blockchain : le pont du droit international privé entre l'espace numérique et l'espace physique," in Ilaria Pretelli (ed), *Conflict of Laws in the Maze of Digital Platforms* (Genève/Zürich: Schultness Editions Romandes, 2018), 164 et seq.; Fabienne Jault-Seseke, "La blockchain au prisme du droit international privé, quelques remarques" (2018) Dalloz IP/IT, 544; Edouard Treppoz, "Quelle régulation internationale pour la blockchain ? Code is law v. Law will become Code," in Franck Marmoz (ed), *La blockchain : big bang de la relation contractuelle* (Dalloz, 2019), 55 et seq.; Thibault Douville, "Blockchains et droit international privé : état sommaire des questions" (2019) 2 Revue de droit international d'Assas, 19; Mathias Audit, "La blockchain et les crypto-monnaies," in Martine Béhars-Touchais (ed), *La blockchain saisie par le droit* (IRJS Editions 2019), vol. 1, 53 et seq. and Audit (n 1) ; Caroline Kleiner, "Aspects

© DAVID SINDRES, 2023 | DOI:10.1163/9789004514850_006
This is an open access chapter distributed under the terms of the CC BY-NC-ND 4.0 license.

In terms of PIL, two series of issues must be addressed, which albeit distinct, are closely related: first, the ability of PIL to tackle legal relationships involving the use of bitcoins, and second, the implementation of PIL to these relationships. In order to address these issues, a distinction can be drawn between the applicability (2) and the application (3) of PIL to Bitcoin.

2 The Applicability of PIL to Bitcoin

Objections against the applicability of PIL to legal relationships involving the use of bitcoins fall into two main categories. Some of them are based on the idea that these relationships are self-regulated and therefore not subject to any State law (2.1), while others put forward a series of hurdles which would make the implementation of PIL nearly impossible in this realm (2.2).

2.1 *The Thesis of a Self-Regulation of Legal Relationships Involving the Use of Bitcoins*

According to some authors,[3] relationships involving the use of bitcoins are submitted to their own rules, which are distinct and autonomous from State laws. Hence, insofar as PIL's main role is to determine the applicable State law to a given relationship, it would have no reason to intervene here. Even though this thesis is presented in several versions, none of them turns out to be convincing.

Pursuant to one of these versions, the specific technology upon which Bitcoin relies, namely the blockchain, forms a self-regulated system, reluctant, as such, to the application of any State law. A famous formula, which was nevertheless not coined for this purpose, is supposed to epitomise this viewpoint: Code is Law.[4] In other words, the blockchain would be subject to its own

juridiques internationaux. Réflexion renouvelée en raison des 'crypto-monnaies'" (2019) Revue de droit bancaire et financier 4.

3 See for instance, Primavera De Filippi and Aaron Wright, *Blockchain and the Law – The Rule of Code* (Harvard University Press 2018); Simon de Charentenay, "Blockchain et droit: Code is deeply Law" (2017) 39 Gazette du Palais, 15.

4 It is worth noting that this formula, which is constantly cited in studies dedicated to the blockchain and to the Bitcoin, was originally coined by Lawrence Lessig to underline the dangers of a withdrawal of State laws from the cyberspace (Lawrence Lessig, *Code: And Other Laws of Cyberspace* (Basic Books 1999) and Lawrence Lessig, "Code Is Law" (*Harvard Magazine*, 1 January 2000) <https://www.harvardmagazine.com/2000/01/code-is-law-html> accessed 30 June 2023.

non-State body of rules, which would result from the numeric codes underlying its operations.

This thesis is, however, ill-conceived: it is indeed based on the erroneous assumption that the functioning of the blockchain is itself subject to a set of legal rules. Yet, trying to identify such legal rules is as absurd as trying to discover the set of legal rules governing the operation of a mobile phone or a laundry machine. This absurdity stems from a confusion between two types of rules which are, in fact, completely different in nature: technical rules on the one hand, and legal rules on the other.

The distinction between those two categories of rules recalls the difference underlined by legal scholars such as Hans Kelsen between laws of nature and rules of law.[5] Indeed, like laws of nature, technical or technological rules are based on a "causation" relationship between a factual hypothesis and a factual consequence. This kind of rule can be subsumed under the formula "if A is, then B is." An example of a law of nature is thus: "if water is heated to 100 degrees (if A is), then it boils (B is)." Likewise, a technical rule can, for instance, provide that "if one presses a given button (if A is), it turns on the light (B is)," or that "if a person or a group of persons certify a given operation through a certain process (if A is), then this operation is registered in a decentralised ledger (B is)." As shown in these examples, the consequences provided for by laws of nature or technical rules are supposed to necessarily occur in cases where the hypotheses, to which they are tied, arise: these norms describe a fact, a *Sein*; they do not seek to lay down what shall be in a given situation, in other words a *Sollen*. It may well be that the consequences mentioned in such rules do not occur, but in such cases, the rules in question must be considered as erroneous, and therefore invalid.

Contrary to laws of nature and to technical rules, rules of law create a relationship of the type "if A is," then "B shall be -or shall not be." This relationship is therefore not characterised by a mere causation between two facts, but is instead based on the imputation of a chosen consequence to a set of facts. This consequence is moreover presented as a *Sollen* and not as a *Sein*: it indicates what shall occur in a given hypothesis. For instance, Article 1240 of the French Civil Code provides that "Any human action whatsoever which causes harm to another" (if A is) "creates an obligation in the person by whose fault it occurred to make reparation for it" (B shall be). The consequences of the legal rules are

5 Hans Kelsen, *Théorie pure du droit* (Dalloz 1962) translation of the second edition by Charles Eisenmann, Dalloz (LGDJ 1999), 105 et seq. and Hans Kelsen, "Aperçu d'une théorie générale de l'Etat" (1926) Revue de Droit Public 561, 562 et seq.; see also René Capitant, *Introduction à l'étude de l'illicite: L'impératif juridique* (Dalloz 1928), 1–5.

therefore not natural or technical data: they depend on an act of will from the rules' recipients, which may well not occur without depriving the rule of its relevance and of its validity. In sum, rules of law, which aim to model and order facts, would lose their normative dimension if, like rules of nature or technical rules, they limited themselves to describing the reality they seek to model.

Not only is there a difference of nature between technical rules and rules of law, but those rules also have different addressees. Technical rules indeed apply to the objects, and more broadly to the technologies, governed by such rules. Thus, technical rules governing the operation of a laundry machine apply to the laundry machine itself, and those underlying the operation of the blockchain apply to the latter, which is a technology and is therefore not supposed to become a legal category.[6] Contrary to technical rules, legal rules are adopted in order to govern human actions and therefore target subjects of law – whether individuals or organisations of individuals – as well as the relationships that form between them.

Given the distinction between technical rules and legal rules, the formula Code is Law turns out to be completely wrong and misleading despite its recent success: *Code is obviously not Law*.

But if rules of law have no vocation whatsoever to compete with numeric codes in order to govern the technology of the blockchain, they are nonetheless bound to apply to legal relationships between subjects of Law which take place on the blockchain or which, more broadly, entertain a link with this technology.

According to some scholars, these relationships would however not be subject to State laws, but rather to rules stemming from a non-State legal order named the "*lex cryptographica*."[7] However, the close parenthood between the *lex cryptographica* and its famous elder, the *lex mercatoria*, raises some doubt as to its existence as an autonomous legal order. Most of the objections to the

6 The thesis advocated by one author (see Audit (n 1), 681), pursuant to which the blockchain would not yet be a legal category, insofar as it would not, to date, be sufficiently regulated by State laws, seems erroneous to us. Indeed, contrary to such institutions as the registered partnerships, to which it is compared by this author, the blockchain is not, in and of itself, a legal relationship between subjects of Law, but merely a technology. It follows that the transitory difficulty which specialists of PIL had encountered upon the inception of registered partnerships to determine the legal category in which they would fall does not arise for the blockchain: when the issue of characterization occurred regarding registered partnerships, it did not pertain to the process of registration, but rather to the relationship of the partners.

7 See Filippi and Wright (n 3).

lex mercatoria[8] can indeed extend to the idea of a "*lex cryptographica*" since both seem to lack features which are generally considered as characteristic of a legal order.

In this regard, the hypothesis of a *societas cryptographica* raises the same reservations as the thesis of a transnational *societas mercatorum*:[9] people who sell, acquire and use bitcoins come from multiple backgrounds and do so for extremely diverse reasons. Therefore, the mere fact that they are or have been parties to operations involving the use of bitcoins does not make them belong to a specific and autonomous *societas cryptographica.*

Moreover, even if one takes for granted the existence of a *societas cryptographica*, the identification of a set of precise legal rules, whether spontaneous or codified, which would be specific to this society, turns out to be especially difficult.

This so-called society would furthermore be devoid of specific courts and of its own sanctions apparatus. It would at most be able to exclude those of its members in case they have, according to the others, adopted a wrong behaviour. However, it is one thing for a given entity to be able to pronounce the exclusion of some of its members, and another to have the power to force them to accomplish something against their will. Indeed, while many organisations are able to exclude their own members, very few are vested with the power not only to deprive themselves of their members but to exercise a real power of constraint over them.[10] The so-called *societas cryptographica* does not appear to fall within the latter category: for instance, it does not have the power to force one of its members to return a sum of bitcoins it would have received by mistake or fraudulently.[11]

Not only is the existence of a legal order of the *lex cryptographica* highly doubtful, but it is also, at any rate, indifferent to the issue at hand. Indeed, assuming this legal order truly exists, and does not boil down to a doctrinal

8 On these objections, see esp. in the French literature, Paul Lagarde, "Approche critique de la *lex mercatoria*," in *Le droit des relations économiques internationales – études offertes à Berthold Goldman* (Paris: Litec, DL 1982), 125 et seq.; Dominque Bureau, *Les sources informelles du droit dans les relations privées internationales* (Thesis: University of Paris II 1992), 541 et seq.; Sylvain Bollée, *Les méthodes du droit international privé à l'épreuve des sentences arbitrales* (Economica 2004), 105 et seq.; Pierre Mayer, "Le phénomène de la coordination des ordres juridiques étatiques en droit privé" (2007) 327 Recueil des Cours de l'Académie de Droit International, 46 *et seq*.

9 On these reservations, see Lagarde (n 8), 15 *et seq*.

10 See in this regard, Mayer (n 8), 47.

11 Anastasia Sotiropoulou and Stéphanie Ligot, "Legal Challenges of Cryptocurrencies: Isn't It Time to Regulate the Intermediaries?" (2019) 16 European Company and Financial Law Review 5, 652–675, 666.

fantasy, nothing would preclude State legal orders from tackling the legal relationships which would fall within the scope of the *lex cryptographica*. There is, indeed, no difference between the issues raised by the so-called *lex cryptographica* and the problems entailed by other entities which, under a large and pluralistic conception of Law, can be regarded as non-State legal orders.[12] Thus, State legal orders assert their power, and submit to their own rules, corporations, sports club, mafias, scientific societies, sects and so on, even though these social groups have their own organisations, their own rules, and their own decision-making bodies. The same could be said regarding legal relationships forming on the blockchain: the fact that these relationships might be subject to a legal order of the *lex cryptographica* does not exclude the intervention of State legal orders and the implementation by the latter of their own legal rules and sanctions. For instance, in a well-known case, the members of a so-called Decentralised Autonomous Organisation (DAO) had decided, through a vote, that one of them had to return an important amount of cryptocurrency he had received by exploiting a failure in the numeric code governing the operations of the blockchain.[13] Assuming this case is illustrative of a form of self-regulation and of an emerging *lex cryptographica*, nothing would have precluded State legal orders from intervening and from having the final say on the matter. Had their courts been seized by some of the parties involved, they could either have annulled the decision made by the majority of the members of the blockchain, just as they can invalidate the decisions of a general assembly of shareholders, or lent support to their decision by constraining the author of the misappropriation to return the funds on the basis of tort or unjust enrichment, for instance.

The proclamation of the existence of a so-called legal order of the *lex cryptographica* does not, therefore, constitute a valid reason for State legal orders to withdraw from this field: they can, through their judicial and legal apparatus, exert their unequaled power of constraint over the diverse relationships involving the use of bitcoins. One may add that, if they do so, the role ascribed to the *lex cryptographica*, conceived as a set of non-State rules, would be very narrow. Indeed, unlike arbitrators, State courts do not, in general, admit the choice of

12 For a pluralistic conception of legal orders, see esp. Santi Romano, *L'ordinamento giuridico* (2nd edn, Firenze: Sansoni 1946). This essay was translated in French by Lucien François and Pierre Gothot, *L'ordre juridique* (Sirey 1975) re-ed. (Paris: Dalloz 2002), preface by Pierre Mayer.

13 See Samuel Falkon, "The Story of the DAO – Its History and Consequences" (*The Startup*, 24 December 2017) <https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee>; see also Audit (n 1), 674.

a non-State law to govern a contract. The Rome I Regulation[14] thus only allows parties to "[incorporate] by reference into their contract a non-State body of law".[15] In such a case, the chosen law does not apply as a *lex contractus*, but as a set of contract terms. This is the reason for which State courts, when they are confronted with the choice of a non-State law, still have to determine the State law which governs the contract and which determines whether it is valid and binding. It follows that, even if the *lex cryptographica* were considered as a relevant non-State body of law, this would not exempt State courts from identifying the applicable State law through their conflict-of-laws rules.

On balance, neither the thesis that Code is Law, nor the existence of the so-called *lex cryptographica* justifies any withdrawal of State laws from the field of relationships involving the use of bitcoins. Insofar as these relationships can be subject to State laws, PIL, whose main role is to determine the applicable State law, has undeniably a role to play in this realm.

Some authors have nevertheless pointed out several hurdles which, they believe, would make the implementation of PIL nearly impossible in practice.

2.2 *The Existence of Hurdles to the Implementation of PIL*

Impediments to the implementation of PIL with respect to relationships involving the use of bitcoins are well-known: they result, on the one hand, from the impossibility to situate these relationships in the physical space and, on the other hand, from the pseudonymity of the parties.

Challenges posed to PIL by relationships which cannot, or at least cannot easily, be localised from a spatial viewpoint are, however, nothing new. These challenges had already been emphasised with the development of the Internet,[16] which is today the vector of very diverse legal relationships, extending from electronic contracts to cyber-torts. Even before the Internet age, similar

14 Regulation (EC) No 593/2008 of 17 June 2008 on the law applicable to contractual obligations (Rome I), [2008] OJ L177/6 ("Rome I Regulation").

15 *Id.*, Recital 13: "This Regulation does not preclude parties from incorporating by reference into their contract a non-State body of law or an international convention." See also, condemning the choice of a non-State law as the law of the contract, Court of Cassation, Civil Chamber 1, 17 May 2017, 15–28.767, Unpublished, Revue critique du droit international privé 2017.431, note D. Sindres; Dalloz 2018, 966, obs. S. Clavel and F. Jault-Seseke; Court of Cassation, Social Chamber, 13 January 2021, 19–17.157, Published in the Bulletin, Dalloz 2021. 139; *id.*, 923, obs. S Clavel et F Jault-Seseke; Droit social 2021. 470, obs. F Jault-Seseke; Revue trimestrielle de droit civil 2021.376, obs. L Usunier.

16 See for instance, in the French literature, Olivier Cachard, *La régulation internationale du marché électronique* (LGDJ 2002), preface by Philippe Fouchard.

problems had appeared with regard to international contracts in general, and contracts concluded by telephone or telex in particular, which, given they are agreements of wills, are abstractions and cannot be tied to one country or another.[17] The same difficulty was also underlined, for instance, with regard to movable properties such as ships or aircrafts. PIL has, however, always managed to cope with these challenges, without having to undergo any major paradigm shift.

There are two main reasons explaining PIL's ability to adapt to situations without any clear localisation in the physical space, or with localisation that proves to be extremely difficult.

First, rules of PIL do not solely aim to localise the legal relationships they govern. Thus, many of these rules give the parties the freedom to choose the competent jurisdiction for their possible disputes[18] and to select the State law applicable thereto.[19] Besides, PIL sometimes resorts to rules which, although based on objective criteria, do not seek to designate the country with the closest links to the matter. In Civil Law countries, for instance, the main rule of jurisdiction is based on the *actor sequitur forum rei* principle: it entitles the claimant to sue the defendant before the courts of the country where the latter is domiciled.[20]

Second, where rules of PIL seek to identify the country with the strongest ties to the matter, they turn out to be flexible enough to adapt to situations which are resistant to any true localisation. PIL has, indeed, never been a "science of observation:"[21] the connecting factors to which it resorts do not seek to reach any exact solution but are rather based on bias lacking any scientific dimension. Under Regulation Brussels I bis, matters relating to contracts are thus, unless otherwise agreed, tied to the place of performance of the obligation on which the claim is based.[22] Regarding the applicable law, the Rome I Regulation provides that, in the absence of choice, contracts are, in principle,

17 Henri Batiffol, *Les conflits de lois en matière de contrats* (Paris: Recueil Sirey 1938), 36; see also Pierre Mayer, «La délocalisation du contrat» in *La relativité du contrat*, Travaux de l'Association Henri Capitant (LGDJ 2000), 123.

18 See for instance, Regulation (EU) No 1215/2012 of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast), [2012] OJ L351/1, art. 25 ("Brussels I bis Regulation").

19 See for instance, Rome I Regulation (n 14), art. 3; Regulation (EC) No 864/2007 of 11 July 2007 on the law applicable to non-contractual obligations (Rome II), [2007] OJ L199/40, art. 14 ("Rome II Regulation").

20 See for instance, Brussels I Regulation (n 18), art. 4.

21 Vincent Heuzé (ed), *La loi des contrats internationaux*, Livre II, Dictionnaire Joly Pratique des contrats internationaux, (Paris: GLN ed. 1989), 32.

22 Brussels I bis Regulation (n 18), art. 7.1.

governed by the law of the country of habitual residence of the party required to effect the characteristic performance of the contract.[23] Like PIL rules pertaining to contractual matters, jurisdiction and conflict-of-law rules relating to tort, delict and quasi-delict can easily adapt to certain damages, such as infringement of personality rights by means of content placed on an internet website, which do not occur in a specific place. When seized with this issue under the Brussels I Regulation, the European Court of Justice thus adopted a flexible solution, pursuant to which the "harmful event" within the meaning of the then-Article 5.3 (now Article 7(2) Brussels I bis) occurs in both the Member State in which the publisher of that content is established, in the Member State in which the victim's center of interests is situated and in each Member State in the territory of which the content placed online is or has been accessible.[24] This type of solution, which amounts to situating the same event in several countries, undeniably bears a fictional aspect. A similar remark can be made regarding the way the *lex rei sitae* is applied to movable properties such as ships, which are submitted to the law of their flag State,[25] or aircrafts, which are subject to the law of their registration State.[26] All these examples bear witness to the fact that PIL rules often resort to flexible solutions based on fiction when it comes to determining the countries with which a given relationship has the strongest ties.

This in turn explains why PIL rules, as demonstrated below,[27] can perfectly be applied to legal relationships involving the use of bitcoins, even though these relationships may prove hard to situate in one country or another.

By contrast, the pseudonymity of the parties raise real and serious issues. It is indeed common knowledge that the identity of each participant in the blockchain is hidden behind two cryptographic keys: a public one, which contains his numeric address, and a private one, which allows its owner to sign off electronically on the operations. This feature of the blockchain

23 Rome I Regulation (n 14), art. 4.

24 See esp. ECJ *eDate advertising GmbH v. X and Société MGN LIMITED* (Joined Cases C-509/09 and C-161/10) [2011] ECR I-10269; ECJ *Bolagsupplysningen OÜ, Ingrid Ilsjan v. Svensk Handel AB* (Case C-194/16) [2017] ECLI:EU:C:2017:766.

25 Court of Cassation, Chambre des Requêtes 6 May 1884, S. 1884.1.337, note Lyon-Caen, Journal du Droit International 1884.512, report Demangeat; aj. Pierre Bonassies, «La loi du pavillon et les conflits de droit maritime» (1969) 128 Recueil des Cours La Haye 1969-III, 505.

26 Convention on the International Recognition of Rights in Aircraft signed at Geneva on 19 June 1948; see also Court of Cassation, Civil Chamber 1, 11 October 1988, 86–15.516, Bull. Civ. I, 288 Revue critique de droit international privé 1991.86, note M. Rémond-Gouilloud.

27 See *infra* sec. 3.

makes it difficult to implement PIL rules for the simple reason that most of these rules require a knowledge of the identity of the parties in order to designate the court which has jurisdiction and the applicable law. For instance, under the Rome I Regulation, the contract is, as seen above, subject, in the absence of choice, to the law of the country where the party required to undertake the characteristic performance of the contract has its habitual residence. In case it would be impossible to identify this party, this conflict-of-laws rule could not be applied.[28]

Despite the fact that it makes it harder to implement PIL rules, the pseudonymity of participants in the blockchain does not, in any manner, justify the withdrawal of these rules from this realm. The problem of pseudonymity is, indeed, just another example of an issue which is consubstantial to Law, and which lies within the practical obstacles, mainly related to proof, on which the application of legal rules frequently stumbles.

This problem shall, however, not be invoked as a pretext for renouncing to the application of rules of law: these rules, which express a *Sollen*, that is a model of behaviour, have never pretended to be completely effective. Moreover, the idea of repealing some of them because of the practical difficulties surrounding their implementation is a dangerous one since it could encourage their addressees to multiply the hurdles to their application in the hope of their abrogation.

We are, furthermore, accustomed to this type of difficulties in Law and have always adopted tools for addressing them. These tools may in turn perfectly apply where there is a need to unveil the identity of the participants in the blockchain.[29] The court may, in this regard, resort to some of the investigative measures provided for by its *lex fori*, and the claimant may also try to establish the identity of the defendant through evidence admissible according to the law of the seized court.[30] A reversal of the burden of proof could also be

28 In the same sense, Audit (n 1), 689.

29 Regulators have already resorted to context discovery, flow analysis, common transactions in a circle of users, and information collected from exchanges to discover the identity of illegitimate users, as in the case of Mt Gox, where Japanese prosecutors charged the head of the exchange with embezzlement amid fraud allegations over the disappearance of hundreds of millions of dollars. See Anastasia Sotiropoulou and Dominique Guégan, "Bitcoin and the challenges for financial regulation" (2017) 12 Capital Markets Law Journal, 466–479, 472.

30 On the applicability of the law of the forum to this issue, see Pierre Mayer, Vincent Heuzé and Benjamin Rémy, *Droit international privé* (12th edn, LGDJ 2019), 193 ; compare with Dominique Bureau and Horatia Muir Watt, *Droit international privé*, (5th edn, Presses Universitaires de France, 2021), 193.

contemplated, pursuant to which it would be up to the party denying ownership of the keys used to perform a given operation to substantiate her claim.

There is, ultimately, no serious objection to the applicability of PIL rules to legal relationships involving the use of bitcoins. It is therefore appropriate to ponder over the ways these relationships can be addressed by both jurisdiction and conflict-of-laws rules.

3 The Application of PIL to Bitcoins

Applying PIL to legal relationships involving the use of bitcoins does not imply the identification of a single law which should govern the blockchain in general. Indeed, as seen above, the blockchain is not a legal category in and of itself. It constitutes a technological medium through which different legal relationships take place, which belong to their own legal categories from a PIL perspective. In this regard, the problem posed by the blockchain to PIL does not differ much from the one which appeared in the wake of the Internet. Indeed, like the blockchain, the Internet is not an autonomous legal category but merely a technology through which multiple legal relationships are formed: electronic contracts, torts, and so on.

The idea here is not to draw up an exhaustive inventory of all the legal relationships on the blockchain or implying the use of bitcoins, but rather to sketch, with a few illustrations, the ways in which PIL can address these types of relationships. In order to do so, a good starting point consists in emphasising the ambivalence of the Bitcoin, which is both a crypto asset and a cryptocurrency. It is therefore possible to study the Bitcoin as an asset on the one hand (3.1) and as a currency on the other (3.2).

3.1 *Bitcoin as an Asset*

Viewed as a crypto asset, the Bitcoin appears as an intangible movable property.

As such, the Bitcoin can be subject to the same operations as any other type of intangible property. It can thus be sold, gifted, exchanged, bequeathed, stolen, diverted, transferred by mistake and so on. A dispute may also arise as to the ownership of this asset.

From a PIL standpoint, these different situations do not, however, raise specific issues: although they relate to bitcoins, they fall within the discipline's traditional categories.

Therefore, a sale of bitcoins can be analysed as an ordinary sale agreement. As such, it may be subject to the rules of jurisdiction applicable to sales of intangible properties which, assuming the contract falls within the scope of

the Brussels I bis Regulation, are to be found in Articles 4, 7(1)(a),[31] as well as Articles 25 or 26 in case the parties have agreed on the competent jurisdiction. As for the applicable law, a sale of bitcoins would, under the Rome I Regulation, be governed by the law chosen by the parties.[32] In the absence of a (valid) choice, the applicable law would be either the law of the country where the seller has his habitual residence[33] or the law of the market, in case the bitcoins are sold through a multilateral system within the meaning of Article 4.1 h.[34]

The observations just made regarding the sale of bitcoins can be transposed to other contractual operations which have bitcoins as their object. Thus, a donation of bitcoins is subject to the rules of PIL governing donation agreements, while exchanges between bitcoins and other assets fall under the rules of PIL applying to exchange contracts. It must also be noted that if the contract giving rise to the dispute is between a consumer and a professional, it may in some cases be subject to PIL rules which are specific to consumer contracts and which can be found in the Brussels I bis Regulation,[35] as far as jurisdiction is concerned, and in the Rome I Regulation, for the applicable law.[36]

Besides, the legacy concerning bitcoins is governed by PIL relating to succession matters. In EU Member States, these rules can be found in the Succession Regulation.[37] Issues of theft and misappropriation of bitcoins are, for their part, included in the tort category and therefore subject to rules of jurisdiction[38] and conflict-of-laws rules[39] relating to this characterisation. The transfer of bitcoins by mistake can either fall within the tort category, when the victim is a third party bringing a claim against the author of the transfer, or within the category of quasi-contract, especially unjust enrichment, when the

31 The option laid down in Article 7.1 b) of the Brussels I bis Regulation (n 18) is not applicable to a sale of bitcoin, since it only covers sales of goods.

32 Rome I Regulation (n 14), art. 3.

33 *Id.*, art. 4(1)(a).

34 Pursuant to *id.*, art. 4(1)(h), "a contract concluded within a multilateral system which brings together or facilitates the bringing together of multiple third-party buying and selling interests in financial instruments, as defined by Article 4(1), point (17) of Directive 2004/39/EC, in accordance with non-discretionary rules and governed by a single law, shall be governed by that law."

35 Brussels I bis Regulation (n 18), section 4.

36 Rome I Regulation (n 14), art. 6.

37 Regulation (EU) No 650/2012 of 4 July 2012 on jurisdiction, applicable law, recognition and enforcement of decisions and acceptance and enforcement of authentic instruments in matters of succession and on the creation of a European Certificate of Succession, [2012] OJ L201/107 ("Succession Regulation").

38 See esp. Brussels I bis Regulation (n 18), arts. 4 and 7.2.

39 See esp. Rome II Regulation (n 19), art. 4.

author of the transfer seeks to retrieve the bitcoins he has transferred by mistake.[40] Finally, disputes relating to the ownership of bitcoins may, when the issue concerns the existence of a transfer of ownership realised by contractual means, be subject to the *lex contractus,*[41] and should otherwise be subject to the *lex rei sitae.*[42]

Although the identification of the relevant rules of PIL turns out to be quite simple, their implementation may prove difficult for the above-mentioned reasons, resulting from the absence of a clear localisation of the operations taking place on the blockchain and from the pseudonymity of the parties involved. Two examples can be used in order to illustrate these difficulties.

First, let us assume a dispute arises between two professionals regarding an international sale of bitcoins. If this dispute falls within the scope of the Brussels I bis Regulation, jurisdiction may be based on several grounds. It can thus result from a prorogation of jurisdiction, in which case the only issue is whether this prorogation is valid and efficient under Article 25 or 26 of this Regulation, regardless of the fact that the sale concerns bitcoins. In the absence of a choice of court by the parties, jurisdiction may result either from Article 4, which designates the courts of the country where the defendant is domiciled, or Article 7(1)(a), which, in matters of contract, allows the claimant to sue the defendant in the court of the place of performance of the obligation that gave rise to the claim. Regarding Article 4, one difficulty may arise insofar as the identification of the country where the defendant is domiciled requires knowledge of the defendant's identity. *Prima facie*, if the claimant has filed a claim against the defendant, he is aware of his identity: otherwise, he could not have summoned him. The defendant might however dispute the fact that he is the owner of the public and private keys through which the operations at the heart of the dispute have been conducted. In such a case, the court may order investigative measures allowed by its *lex fori* and the claimant may himself try to bring evidence as to the identity of the cryptographic keys' owner. As seen above, it is also conceivable to reverse the burden of proof, and to require the defendant to demonstrate that he is not the owner of the cryptographic keys. Other problems may also arise if the claimant decides to use the option laid

40 On the law governing quasi-contracts, see *id.*, arts. 10 and 11.

41 In favour of the application of the *lex contractus*, see Cass. Civ. 1re 21 July 1987, Revue critique de Droit international privé 1988.699, note J Héron ; Dalloz 1988.345, obs. B. Audit. see also Mayer, Heuzé, and Rémy (n 30), 681.

42 Unlike one author's opinion (Jault-Seseke (n 2)), it does not appear relevant to us to reflect upon the law applicable to the ownership of intellectual property rights on bitcoins since the latter can only with difficulty be viewed as a creation of the mind within the meaning of Intellectual property law.

down in Article 7(1)(a). The implementation of this provision indeed requires identifying the place of performance of the obligation underpinning the claim, which can prove impossible when this obligation is performed on the blockchain. However, the ECJ has adopted, under Article 5 (1) of the Brussels Convention, a method of localization which is still relevant today for contracts falling under Article 7 (1) (a) of the Brussels I bis Regulation and which makes it easier to solve this problem: it has indeed ruled that the place of performance of the obligation had to be determined pursuant to the law applicable to this obligation,[43] which usually corresponds to the law of the contract. Assuming the Rome I Regulation is applicable to this contract, the applicable law should either be the one chosen by the parties, or the law of the country of habitual residence of the party required to undertake characteristic performance of the contract. If this party is the claimant, he will reveal his identity. On the contrary, if this party is the defendant, the fact that his identity is hidden behind cryptographic keys may raise the same problems as the ones underlined above.

A second example concerns a claim of ownership of a certain amount of bitcoins. Under the Brussels I bis Regulation, such a claim could be brought either before the court whose jurisdiction has been prorogated by the parties under the conditions of Article 25 or 26, or before the courts of the country where the defendant is domiciled, pursuant to Article 4. Once again, the issue relating to the pseudonymity of the defendant may arise under Article 4. As for the applicable law, it would, in principle, be the *lex rei sitae*. In order to solve the difficulties posed by the impossibility to situate bitcoins in the physical space, one possible solution would be to adopt a fictional localisation, as it is already the case for other properties, such as ships and aircrafts.[44] Bitcoins could, in this regard, be localised at the seat of the company providing the wallet in which they are stored.

As demonstrated through these two examples, PIL rules can adapt to the multiple operations to which Bitcoin gives rise as a crypto asset. These operations may turn out to be difficult to situate in the physical space, but the flexibility of PIL rules helps to solve these difficulties, which are, in any case, not specific to operations involving the use of bitcoins and taking place on the blockchain. The problems resulting from the pseudonymity of the parties is more acute and may seriously complicate the implementation of PIL rules. These problems, which are factual in nature and relate to evidence, are nonetheless not specific to PIL. Moreover, they could be solved thanks to

43 See ECJ *Industrie Tessili Italiana Como v. Dunlop AG* (Case 12/76) [1976] ECR 1976-01473.

44 See *supra* sec. 2.2.

the methods to which courts generally resort when it proves necessary to lift secrecy.

Besides being an asset, Bitcoin is also a currency which, as such, raises specific problems under PIL.

3.2 *Bitcoin as a Currency*

As a cryptocurrency, Bitcoin aims at competing with traditional State currencies.

In this regard, the main question is whether Bitcoin can, from a legal standpoint, achieve this ambition and appear as a true document currency on the one hand, and as a true payment currency on the other hand.[45]

The answer to this question is, nonetheless, not to be found in PIL, whose role is to identify the body of substantive rules pursuant to which this problem shall be solved.

To identify this set of substantive rules, a first step is to determine in which legal category Bitcoin should be included from a PIL perspective. The fact that some State laws are reluctant to consider cryptocurrencies in general, and Bitcoin in particular, as a currency, is not a reason for discarding such a characterisation under PIL. Indeed, legal categories in PIL are not, contrary to the ideas of Bartin,[46] mere projections of legal categories used in the substantive law of the forum: they turn out to be broader than the latter in order to include institutions which, albeit distinct from their counterparts in the substantive law of the forum, share with them characteristic features. The way PIL deals with the institution of marriage exemplifies this idea: in countries such as France where polygamy is banned, polygamous marriages nonetheless fall in the marriage category when it comes to resolving conflicts of laws.[47] The reason why legal categories in PIL are broader than legal categories of substantive law is that PIL is a meta-Law, which does not aim to determine the rights and obligations of private parties, but to identify the law which provides for these rights and obligations. PIL must therefore be flexible and display open-mindedness: this is the *conditio sine qua non* of an efficient approach to legal and cultural diversity.

---

45 On the distinction between document currency and payment currency, see in the French literature Edmond de la Marnierre, *Monnaie de compte et monnaie de paiement* (1951), 169.

46 See esp. Étienne Bartin, «De l'impossibilité d'arriver à la suppression définitive des conflits de lois» (1897) 24 Journal Dr. Int'l Prive & Juris. Comparee, 225, 466, and 720.

47 See for instance, Court of Cassation, Civil Chamber 1, of 3 January 1980, 78–13.762, Bull. Civ. I, no. 4, Revue Critique de droit international privé 1980.331, note H. Batiffol; Journal du Droit International 1980.327, note M. Simon-Depitre, D. 1980.549, note E. Poisson-Drocourt, GAJDIP (5th edn, Dalloz 2006), no. 61.

This flexibility is, however, not without limits. In particular, it shall not lead to retain an obviously inadequate characterisation. For instance, it was inappropriate to include registered partnerships, upon their inception, in the marriage category since they had been created as an alternate solution for those who did not wish to or could not marry.

That said, characterising Bitcoin as a currency within the meaning of PIL would not, in our view, amount to committing such a mistake. Indeed, Bitcoin aims to compete with traditional State currencies by reproducing their main functions and thus presents itself as a currency. True, it is a new kind of currency, allegedly more efficient and secure than traditional currencies,[48] but it is still a currency.[49]

Accordingly, it would seem reasonable for us to consider Bitcoin as a currency from a PIL perspective, unless the connecting factors corresponding to this categorisation prove manifestly ill-suited to Bitcoin.

To determine whether this is the case, a distinction shall be drawn between two distinct categories: "document currency" on the one hand, and "payment currency" on the other.

The document currency serves to fix the amount of a given obligation. Under PIL, it is generally considered to be subject to the law governing the obligation it serves to evaluate. Given the fact that this obligation usually results from a contract, the law applicable to the document currency is, in principle, the *lex contractus*.[50] Accordingly, it is up to the law governing the contract to determine whether the parties to an international sale or to an international

48 Sotiropoulou and Ligot (n 11), 657.

49 The European Court of Justice has taken notice of Bitcoin's ambition: in the *Skatteverket v. David Hedqvist* decision (Judgment of the Court (Fifth Chamber) of 22 October 2015 *Skatteverket v David Hedqvist*, *aff.* C-264/14, ECLI:EU:C:2015:718), the Court underlined that "it is common ground that the 'bitcoin' virtual currency has no other purpose than to be a means of payment and that it is accepted for that purpose by certain operators" (para. 52). This assertion is nonetheless too strong and radical: although Bitcoin aims at competing with State currencies as a means of payment, it can also play a role as a document currency and as an investment asset. On the role of Bitcoin as an investment asset and the risks it poses, see Sotiropoulou and Ligot (n 11).

50 See Henri Batiffol and Paul Lagarde, *Droit international privé* (7th edn, LGDJ 1983), vol. 2, 613; see also, Henri Batiffol, note on the Court of Cassation, Civil Chamber 1, 24 April 1952, Revue critique de Droit international privé 1952.502; see also Mayer, Heuzé, and Rémy (n 30), 793; compare with Kleiner (n 3), 341 et seq.; see also in French caselaw, Court of Cassation, Civil Chamber 21 June 1950, Messageries maritimes, Revue critique de Droit international privé 1950.609, note H. Batiffol, JCP 1950.II.5812, note J-Ph. Lévy; Dalloz 1951.749, note Hamel; S.1952.1.1, note Niboyet; GAJDIP cited above no. 22; Cour de Cassation Civil Chamber 1, 15 February 1972, Revue critique de Droit international privé 1973.77, note H. Batiffol.

services contract are entitled to resort to Bitcoin to determine the value of the properties sold or the services provided.

Besides conflict-of-law rules, some State laws have adopted international substantive rules governing the choice of the document currency. Under French PIL, for instance, the *Cour de cassation* has, in the landmark *Messageries maritimes* case,[51] upheld a "gold clause" stipulated in an international loan agreement, thereby paving the way to the freedom of choice of the document currency by parties to international contracts.[52] In cases where French law, or another State law containing a similar international substantive rule, is applicable to the contract, one may wonder whether the parties' freedom of choice of the document currency extends to cryptocurrencies. In our view, a positive answer is possible since the *ratio legis* of this rule is to provide parties to international contracts with extensive freedom as to the choice of the document currency. Moreover, if parties are allowed to insert gold clauses in their contracts, which allow the creditor to receive payment in gold or gold equivalent, there is no reason to deprive them of the possibility to opt for a cryptocurrency such as Bitcoin which, unlike gold, pretends to be not only an asset, but also a money.

The identification of the law applicable to the payment currency turns out to be more difficult than the determination of the law governing the choice of the document currency: one may indeed hesitate between the *lex contractus* and the law of the country where the payment is supposed to occur.[53] If the latter solution is retained, as is the case under Swiss PIL,[54] and maybe also under French PIL,[55] its implementation to payment in bitcoins would raise two difficulties.

The first one would stem from the fact that the identification of the place of payment is especially difficult regarding bitcoins, since there is neither a physical delivery of the funds nor any bank account on which the bitcoins are wired. To overcome this difficulty, one possible solution could be to determine the

51 Civ. 21 June 1950 (n 49).

52 This principle has since been reaffirmed by French courts. See esp. Court of Cassation, Civil Chamber 1, 11 October 1989, 87–16.341, Bull. Civ. I, no. 311; Dalloz 1990.167, note E.S. de la Marnierre; JCP 1990.II.21393, note J.-Ph. Lévy.

53 See in this regard, Dominique Carreau and Caroline Kleiner, «Monnaie » in *Répertoire de droit international* (Paris: Dalloz 2017), 119 *et seq*.

54 Article 147, para. 3 of the Swiss Federal Act on Private International Law (PILA) provides that "[t]he law of the state in which payment must be made determines the currency in which the payment must be effected." Swiss Federal Act on Private International Law (PILA) of 18 December 1987, RS 291.

55 See Mayer, Heuzé, and Rémy (n 30), 797.

place of payment according to the law governing the obligation in exchange of which the payment shall be made.[56] This law may in turn require a payment at the creditor's domicile, or at the debtor's domicile. It may also enable the parties to choose the place of payment, and provide for a suppletive rule according to which the payment shall, in the absence of choice, intervene either at the debtor's or at the creditor's domicile.[57]

The second difficulty would result from some provisions of State laws which prohibit or at least limit the possibility of making payments in foreign currencies. Under French law for instance, Article 1343-3 of the Civil Code states that "payment in France of monetary obligations must be made in euros." However, it adds that "payment may be made in another currency if the obligation providing for it arises from a transaction of an international character or from a foreign judgment." Article 1343-3 also enables the parties to "agree that payment should be made in a foreign currency if it is to be effected between persons acting in the course of business or a profession and where use of a foreign currency is commonly accepted for the transaction in question." Assuming this provision would be applicable on the ground that the payment should intervene in France pursuant to the law governing the obligation in return for which the payment is made, the principle would be that a payment in bitcoins would be forbidden, since it has to be made in euros. Would a payment in bitcoins also be prohibited if it were to intervene in the framework of an international transaction within the meaning of Article 1343-3 of the Civil Code? The answer would depend on whether Bitcoin can be viewed as "another currency" under this provision. The fact that Bitcoin may be considered a currency from a PIL perspective does not necessarily imply that the same characterisation must be adopted with respect to substantive rules: the two characterisations may, indeed, differ.[58] In the absence of any clue resulting from the law itself, it would be up to the courts of the forum to decide whether Bitcoin may be characterised as "another currency" within the meaning of Article 1343-3 of the Civil Code. In this regard, it must be noted that courts are not bound by the

56 See Audit (n 1), 684.

57 Article 1343-4 of the French Civil Code provides that "Unless legislation, the contract or the court otherwise provide, the place of satisfaction of a monetary obligation is the domicile of the creditor."

58 On the necessity to operate a double characterisation, first at the stage of the implementation of the conflict-of-laws rules, and second, within the body of substantive rules designated by the conflict-of-laws rules of the forum, see Mayer, Heuzé, and Rémy (n 30), 163.

often-hostile stance taken by central banks with respect to the characterisation of Bitcoin as a currency.[59]

It is, however, important to avoid any misunderstanding as to the stake of such a characterisation: it relates only to the ability of the debtor to unilaterally impose a payment in bitcoins on the creditor.[60] On the other hand, if the parties have agreed that the payment of a given monetary obligation should intervene in bitcoins, the only issue is whether the law of the payment authorises such an agreement and, if so, under which conditions.[61]

Assuming French law would be applicable, such an agreement would surely be valid if Bitcoin were characterised as a "foreign currency" within the meaning of Article 1343-3 of the Civil Code. True, this provision lays down limits as to the parties' freedom to agree that the payment should intervene in a foreign currency: as seen above, such an agreement is only valid if the payment is to be made between professionals and provided that a foreign currency is commonly accepted for the transaction in question. However, it results from the way Article 1343-3 is drafted that these limits only apply to internal transactions. On the contrary, the parties' freedom shall prevail as far as international transactions are concerned. Indeed, insofar as Article 1343-3 allows the debtor to impose a payment in a foreign currency on the creditor in the context of an international transaction, parties to such a transaction should not be denied the right to agree that the payment should intervene in a foreign currency: who can do the most can do the least.

---

59 *Contra* Audit (n 1), 683. The author advocates that, insofar as neither the French central bank nor the European Central Bank have accepted considering cryptocurrencies as currencies, the reference to "other currencies" found in Article 1343-3 cannot be interpreted as encompassing cryptocurrencies.

60 In the same sense, Audit (n 1), 683.

61 Unlike one author's opinion (Audit (n 1), 684), it seems impossible to us to interpret the ECJ's decision in the *Skatteverket* (n 49) case as authorising in the EU Member States agreements providing for a payment in bitcoins or in another cryptocurrency. The questions referred to the ECJ in this case were indeed solely as to whether transactions which consist of the exchange of traditional currency for units of bitcoins and vice versa were liable to VAT. True, the Court notes that "it is common ground that the 'bitcoin' virtual currency has no other purpose than to be a means of payment and that it is accepted for that purpose by certain operators" (para. 52), but this assertion must not be construed out of context. It came as a justification for including exchanges of traditional currency against bitcoins among supplies of services within the meaning of Article 135, para. 1(e) of the Directive 2006/112/EC of 28 November 2006 on the common system of value added tax, [2006] OJ L347/1. Moreover, if the ECJ observes that bitcoin is accepted as a means of payments by certain operators, it does not take any stance as to the lawfulness of the contracts by which the parties would agree to a payment in bitcoins.

One may finally wonder what the solution would be if Bitcoin were not characterised as a "foreign currency" within the meaning of Article 1343-3 of the Civil Code. Would that imply that an agreement by which the parties select Bitcoin as the payment currency would be unlawful under French law? Not necessarily: as underlined above, Bitcoin is hybrid in nature since it is both a cryptocurrency and a crypto asset. Thus, if Bitcoin could not be characterised as a currency under the applicable substantive law, it could still be possible to consider it as an asset. In such a case, a contract by which the parties would agree that the payment of any given monetary obligation should be made in bitcoins could be characterised either as an exchange contract, where the payment of bitcoin would be made in exchange for a property, or as a service contract if the bitcoins were to appear as a consideration for the supply of a service. Unless the State law governing the payment, applicable through the relevant conflict-of-laws rule of the forum or as an international mandatory rule ("loi de police"), would expressly prohibit the use of bitcoins as the consideration for the delivery of a property or for the performance of a service, there would be no reason to consider such agreements as unlawful.

• • •

Challenges posed by Bitcoin to PIL must ultimately not be overstated. The thesis of a self-regulation of legal relationships involving the use of Bitcoin is fragile and, if true, does not imply the eviction of PIL rules: these rules can, and indeed, apply to many relationships which are also governed by their own set of non-State laws. Moreover, even though there may be practical hurdles to the implementation of PIL to these relationships, they are rather banal and can all be overcome without having to introduce sweeping changes to current conflict-of-laws and conflict-of-jurisdictions rules. Finally, the main question raised by Bitcoin from a PIL perspective seems to be less a technical or methodological one than a Shakespearian one: much ado about nothing?

CHAPTER 5

Proprietary Rights in Digital Assets and the Conflict of Laws

Christiane Wendehorst

Digital assets – from raw data to software to Bitcoin – are among the most valuable assets in our modern economies. Their sheer variety and their novelty pose challenges not only for substantive law, but also for conflict of laws.[1] This is partly due to the speed of technological progress, but also to grey areas between the law of obligations, intellectual property law, (tangible) property law and a range of overriding mandatory provisions of a more regulatory nature, which results in a challenge for both classification and the identification of the most appropriate connecting factor(s). While the contractual aspects of transactions may be covered by the Rome I Regulation[2] and similar conflict-of-laws legislation outside the EU, including the 2015 Hague Principles on Choice of Law in International Commercial Contracts,[3] the proprietary aspects are still very much unchartered territory. This includes, for example, the question of who has rights in crypto assets that take effect vis-à-vis third parties and how such rights can be assigned, with assignment meaning anything from full transfer of title to transfer of title by way of security to the

1 Christiane Wendehorst, "Digitalgüter im Internationalen Privatrecht," (2020) Practice of Private International and Procedural Law 6, 490; Christiane Wendehorst, "Art. 43 EGBGB," in Franz Jürgen Säcker et al. (eds), *Münchener Kommentar zum Bürgerlichen Gesetzbuch*, vol. 12, (8th edn 2020), n. 261 et seqq.; Matthias Lehmann, "Who Owns Bitcoin? Private Law Facing the Blockchain," (2019) 21 Minnesota Journal of Law, Science & Technology 93; Florence Guillaume, "Aspects of Private International Law Related to Blockchain Transactions," in Daniel Kraus, Thierry Obrist and Olivier Hari (eds), *Blockchains, Decentralised Autonomous Organisations and the Law* (Edward Elgar 2019), 49 ff; Björn Steinrötter, "International Jurisdiction and Applicable Law," in Philip Maume, Lena Maute and Mathias Fromberger (eds), *The Law of Crypto Assets*, (C.H. Beck 2022), 69.

2 Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), [2008] OJ L177/6 ("Rome I Regulation").

3 The *Principles on Choice of Law in International Commercial Contracts* (Choice of Law Principles) are the first 'soft-law' instrument of the HCCH, available at Hague Conference on Private International Law (HCCH), "40: Principles on Choice of Law in International Commercial Contracts" (*HCCH*, 2015) <https://www.hcch.net/en/instruments/conventions/full-text/?cid=135> accessed 15 March 2023.

© CHRISTIANE WENDEHORST, 2023 | DOI:10.1163/9789004514850_007
This is an open access chapter distributed under the terms of the CC BY-NC-ND 4.0 license.

provision of a security interest such as a pledge. Rights that take effect vis-à-vis third parties may be akin to ownership, but they may also be of a very different, data-specific nature. Recently, the debate has focused on crypto assets, but it seems worthwhile to set the broader scene of digital assets in general.

1 Digital Assets and Other Digital Phenomena

There is no generally recognised definition of what counts as a 'digital asset'.[4] Generally speaking, digital assets are items consisting of, or represented by, digital data, which are subject to a person's control.[5] The notion of 'digital' is to be understood broadly, and includes phenomena such as analogous or quantum computing. What is more difficult to define is 'control'. Arguably, at this very abstract level of delineating the topic, control should be understood primarily as a factual concept, which refers to a degree of factual influence or power a person has over a digital asset, such as by being able to use it or to enable others to use it.[6] This does not exclude in any way that control may normally correlate with legal authority (such as where access to an asset requires authentication

4 For an overview, see United Nations Commission on International Trade Law (UNCITRAL), "Legal issues relating to the digital economy – digital assets" (*UN*, 12 May 2020) <https://documents-dds-ny.un.org/doc/UNDOC/GEN/V20/025/48/PDF/V2002548.pdf?OpenElement>.

5 See the more elaborate definition used by the 2022 ELI Principles on the Use of Digital Assets as Security: "'digital asset' means any record or representation of value that fulfils the following criteria: (i) it is exclusively stored, displayed and administered electronically, on or through a virtual platform or database, including where it is a record or representation of a real-world, tradeable asset, and whether or not the digital asset itself is held directly or through an account with an intermediary; (ii) it is capable of being subject to a right of control, enjoyment or use, regardless of whether such rights are legally characterised as being of a proprietary, obligational or other nature; and (iii) it is capable of being transferred from one party to another, including by way of voluntary disposition." European Law Institute, "ELI Principles on the Use of Digital Assets as Security" (*ELI*, 2022) <https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_the_Use_of_Digital_Assets_as_Security.pdf> accessed 15 March 2023.

6 See draft Principle 6(1) of the International Institute for the Unification of Private Law (UNIDROIT) Working Group on Digital Assets and Private Law, "Working Document Study LXXXII – W.G.8 – Doc. 2" (*UNIDROIT*, March 2023), discussed at the Working Group meeting 8 to 10 March 2023 <https://www.unidroit.org/wp-content/uploads/2023/03/W.G.8-Doc.-2-Draft-Principles-and-Commentary-Clean.pdf> accessed 15 March 2023: "(1) A person has 'control' of a digital asset if: (a) […] the digital asset or the relevant protocol or system confers on that person: (i) the exclusive ability to change the control of the digital asset to another person …; (ii) the ability to obtain substantially all the benefit from the digital asset; and (iii) the exclusive ability to transfer the abilities in sub-paragraphs (a)(i), (a)(ii) and (a)(iii) to another person […] (b) the digital asset or its associated records allows that person to identify itself as having the abilities set out in paragraph (1)(a)."

and the key is provided only to the rightful holder) and/or may depend on a particular legal relationship (such as an account held with a platform operator).[7] For particular purposes, such as perfection of a security interest, more specific notions of 'control' may need to be introduced.Looking at the landscape of digital phenomena fulfilling these conditions, it becomes clear that the relevant phenomena differ widely, which makes it difficult to imagine that there could be a uniform conflict rule for all digital assets in the broader sense. Rather, the first step must be some sort of classification, grouping digital assets into different categories that are meaningful for the purposes of a conflict-of-laws analysis. One meaningful way of classifying digital assets into different categories is putting a focus on the extent to which assets are of a rival or non-rival nature. 'Rivalrousness' is understood in this paper as referring to the possibility of duplicating an asset at will, and at basically no cost or delay, so that it can be used by multiple parties without being exhausted. Even where a resource is non-rival, such as a particular intellectual achievement, the law can afford a party the exclusive right to use it or to allow others to use it (legal exclusivity), or a party can apply technical measures to protect a resource from being used by others (technical exclusivity). The following table identifies five different categories of assets, relying on their relative degree of rivalrousness and/or exclusivity.

TABLE 5.1 Categories of assets

1a	**1b**	**2a**	**2b**	**3**
Duplication technically and legally possible for anyone in control	Duplication technically possible for anyone in control, but rightholder's consent required	Duplication technically and legally possible for rightholder/ system owner	Duplication technically possible for system owner, but legally binding promise not to duplicate	Duplication technically impossible, even for system owner.
Example: raw IoT data	*Example: software, book manuscript*	*Example: copy-protected e-book*	*Example: tradeable in-game equipment*	*Example: cryptocurrencies*

7 The ELI Principles (n 5) use a hybrid concept instead: "'control' in respect of a digital asset means the legal power or factual capability of any natural or legal person to deal in and/or extinguish such assets, as the case may be." However, for perfection and some other purposes, only factual control counts; see *id.* at 20.

The category of assets that most obviously requires analysis from a proprietary rights point of view, and that most obviously requires appropriate conflict rules for such rights, is category 3. In particular, it comprises crypto-assets and similar fully rival assets.

2 Crypto Assets – The General Background

2.1 *Distributed Ledger Technology* (*DLT*)

Data (or electronic records) can represent assets that cannot be duplicated and can only be allocated to one person at a time (or to several persons jointly), *i.e.*, that are fully rival, and that can be subject to exclusive control. Where data fulfils these conditions it can in principle qualify as a form of 'property' under many legal systems in the world.[8] In recent years, the discussion has focused on 'virtual currencies', 'coins', 'tokens', and similar phenomena. In order to represent rival assets, there must be a technical solution to the problem of 'double spending', which is achieved through a series of cryptographic procedures. Therefore, such assets are commonly referred to as 'crypto assets', 'cryptocurrencies', *etc.* The 2020 Proposal for a Regulation on Markets in Crypto-assets (MiCA)[9] defines the term 'crypto-asset' as meaning a digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology. As the individual units only exist virtually, they are fully dependent on some kind of digital platform or ledger on which they are recorded and transferred. The AMLD IV[10] (as amended by the AMLD V[11]) defines 'virtual currencies' as a digital representation of value

8 For instance, data may qualify as a 'bien' pursuant to the French Civil Code, arts. 516 et seqq. or as a 'Sache' pursuant to the Austrian Civil Code, art. 285.

9 Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, [2020] COM/2020/593 final ("MiCA Proposal").

10 Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, [2015] OJ L141/73 (Anti-money laundering Directive IV; "AMLD IV").

11 Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, [2018] OJ L156/43 (Anti-money laundering Directive V; "AMLD V").

that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically. Strictly speaking, this definition is a little outdated since sovereign states, such Ecuador and the Central African Republic, have recognised Bitcoin as legal tender.

Because centralised systems, where a system operator could theoretically switch off or manipulate the system, would reduce their value as property, crypto assets usually exist on distributed ledgers, in particular blockchains, which also allow for appropriate cryptography. Distributed ledger technology (DLT) is characterised by the fact that certain desired properties of a booking system – in particular protection against subsequent tampering or damage as well as independence from a central instance – are achieved by a large number of computers ('nodes') having each stored the identical data record. This requires constant synchronisation between the computers and a consensus mechanism, *i.e.*, a procedure with the help of which a 'correct' data record is identified and finally adopted by all computers in the network. The 'proof of work' approach of the Bitcoin blockchain is just one of many ways of designing the consensus mechanism, in which so-called 'miners' solve a task at the cost of considerable computing power and are rewarded with new bitcoin if they win the validation race. Other popular consensus mechanisms include 'proof of authority' and 'proof of stake'. The latter has been announced as Ethereum's future consensus mechanism, which will leave validation to the nodes that have 'locked up' the highest amount of Ether.[12]

Tokens are called 'fungible' tokens where they are exchangeable against other tokens of the same class because each token of that class represents a right or value of the same kind, and they can usually be divided into fractions. By contrast, so-called 'non-fungible tokens' (NFTs) are uniquely identified and thus suitable for the representation of (rights in) unique objects existing outside the ledger, such as a painting or a diamond, or of (rights in) objects existing on a different ledger (distributed or not), like a piece of digital art.[13]

12 Dirk Siegel, "Technische Grundlagen," in Sebastian Omlor and Mathias Link (eds), *Kryptowährungen und Token* (1st edn, Recht und Wirtschaft 2021), 101.

13 Sebastian Omlor, "Allgemeines Privatrecht," in Sebastian Omlor and Mathias Link (eds), *Kryptowährungen und Token* (1st edn, Recht und Wirtschaft 2021), 257.

2.2 *Endogenous and Exogenous Tokens*

A central distinction is that between endogenous tokens and exogenous tokens.[14] Endogenous tokens represent a value that only exists within the ledger. Theoretically, they serve payment purposes and are often referred to as 'payment tokens', 'currency tokens' or 'coins', but in reality, they are objects of speculation, as investors buy them with the expectation that their value will rise over time. Bitcoin and Ether are the two most famous types of endogenous tokens. While Bitcoin and some other endogenous tokens exist on their own blockchain, most payment tokens exist on larger platforms that host a range of different tokens or applications, such as the Ethereum blockchain. As the high volatility of most payment tokens make them attractive for high-risk investment, but unattractive as an alternative means of payment, so-called 'stablecoins' have been introduced, whose value does not oscillate to the same extent. The 2020 MiCA Proposal defines 'asset-referenced token' as a type of crypto asset that purports to maintain a stable value by referring to the value of several fiat currencies that are legal tender, one or several commodities, one or several crypto assets or a combination of such assets.[15]

Exogenous tokens, on the other hand, are tokens representing rights that exist outside the ledger, be it claims of any sort, shares in a company or property rights. A line is drawn between so-called 'security tokens' and 'utility tokens', with the latter functioning like digital vouchers and providing digital access to a good or service supplied by the issuer of that token.[16] The creation of a link between the digital representation on DLT and the represented right is called 'tokenisation'. It is comparable to the process of creating traditional securities. Like with traditional securities, the issuer can create the rights and the tokens at the same time, such as by promising to grant certain rights to anyone holding the token, or it can 'tokenise' already existing assets. For the purpose of conflict of laws, exogenous tokens pose particular problems because there are two assets involved: the digital asset and the asset the digital asset represents.[17]

Furthermore, some differentiate, for exogenous tokens, between so-called 'token ledgers' or 'title ledgers' on the one hand and mere 'record ledgers' on

14 Stefan Möllenkamp and Leonid Shmatenko, "Blockchain und Kryptowährungen," in Thomas Hoeren, Ulrich Sieber and Bernd Holznagel (eds), *Handbuch Multimedia-Recht* (Werkstand 50, October 2019), n. 29 *et seq*.

15 MiCA Proposal (n 9), art. 3(1)(3).

16 Armin Varmaz et al., "Rechtliche und finanzökonomische Grundlagen," in Sebastian Omlor and Mathias Link (eds), *Kryptowährungen und Token* (1st edn, Recht und Wirtschaft 2021), 21 *et seq*.

17 Wendehorst, "Art. 43 EGBGB" (n 1), n. 310.

the other hand.[18] The idea of a title ledger is that, theoretically, proprietary rights regarding the represented asset should follow proprietary rights regarding the token, mirroring the situation with certificated or book-entry securities. Conversely, in the case of a mere record ledger, transactions with proprietary effect occur exclusively or primarily outside the ledger according to the law governing the represented asset, and the only asset in which there exist any independent proprietary right is the represented asset.

2.3 *The Necessity of Assigning Proprietary Rights in Crypto Assets*

Various types of crypto assets have become popular objects of speculation for both private and professional investors, and in some cases such assets account for a significant share of a natural or legal person's estate.[19] Consequently, digital assets may serve similar purposes as traditional classes of assets. For instance, crypto assets may be used as collateral to secure a loan, necessitating the determination of the applicable law for the effective provision of security interests.[20] Furthermore, in the event of a natural or legal person's default or bankruptcy, crypto assets 'belong' to the debtor's bankruptcy estate and thus may be liquidated for the satisfaction of creditors. In many cases, the transfer of ownership in crypto assets may take place outside the ledger. This becomes particularly clear in the case of intestate succession. The heirs acquire ownership of digital assets although they will very likely not be in actual (albeit possibly fictional) possession of public and private keys.[21] Most transfers of ownership, however, occur by means of voluntary transactions on the ledger or accompanied by a booking on the ledger.

3 Special Conflict Rules for Proprietary Rights in Crypto Assets

If it is necessary to assign proprietary rights in crypto assets to particular parties, and to do this in a way that provides both fairness and certainty, the first question that arises is the one of which is the governing law.

---

18 Financial Markets Law Committee, "Distributed Ledger Technology and Governing Law: Issues of Legal Uncertainty" (FMLC, March 2018), 8, <http://fmlc.org/wp-content/uploads/2018/05/dlt_paper.pdf>.

19 Even publicly listed companies invest their capital in cryptocurrencies (cf. "Elon Musk's Tesla buys $1.5bn of Bitcoin causing currency to spike" (*BBC*, 8 February 2021) <https://www.bbc.com/news/business-55939972>).

20 Koji Takahashi, "Implications of the Blockchain Technology for the UNCITRAL Works" (*SSRN*, 31 July 2017), 84 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3566691>; see also the European Law Institute (n 5).

21 Lehmann (n 1), 130.

3.1 *Selected National Legislation*

Since existing property laws and PIL rules struggle to cover all kinds of crypto assets, some countries have decided to implement specific laws to tackle these issues. However, to date, only few conflict rules exist regarding the law applicable to proprietary interests in crypto assets and similar digital assets, and many of them are mere soft law. The following overview is far from being complete and just highlights some selected approaches.

3.1.1 Liechtenstein

The Liechtenstein Law of 3 October 2019 on Tokens and VT Service Providers (*Token and VT Service Provider Act; TVTG*)[22] was one of the first well developed regulatory models in Europe.[23] According to its Article 3, the TVTG governs the legal qualification of tokens and token transfers, including with regard to third-party effects, if tokens are generated or issued by a VT Service Provider with its headquarters or place of residence in Liechtenstein, or where the parties to a transaction choose Liechtenstein law to apply in a legal transaction over tokens. The latter is particularly remarkable, as it allows parties with no connection whatsoever to the territory of Liechtenstein to subject their transaction to the laws of Liechtenstein, including regarding aspects affecting third parties. The TVTG includes a rule in Article 6 stating the requirements for a transfer or granting of a right in rem having third-party effects, with Articles 7 and 8 addressing the effects of the transfer or granting of right in rem and Article 9 dealing with *bona fide* purchase.

3.1.2 Switzerland

In 2020, Switzerland adapted its legal system to some of the challenges associated with DLT.[24] With regard to conflict of laws, a very cautious approach was taken. Basically, the new Sec. 145a, which was inserted into the 1987 Federal Act on Private International Law, states that the question of whether a claim is represented by a title in paper or equivalent form (including DLT) and transferred by means of that title is determined by the law designated therein. Swiss law therefore allows for choice of a particular law for the whole DLT system. If no law is specified in the title, the law of the country in which the issuer has its

22 Law of 3 October 2019 on Tokens and VT Service Providers Act, Liechtensteinisches Landesgesetzblatt, 2019, No. 301 (Token- und VT-Dienstleister-Gesetz; "TVTG").

23 Sarah Lorraine Wild, *Zivilrecht und Token-Ökonomie in Liechtenstein* (Verlag Österreich, 9 October 2020), 1; see also Nicolas Raschauer and Rainer Silbernagl, "Grundsatzfragen des liechtensteinischen 'Blockchain-Gesetzes' - TVTG," (2020) ZFR 2020/3, 11.

24 Federal Act of 25 September 2020 adapting federal law to developments with regard to distributed ledger technologies, in force since 1 February 2021, AS 2021 33; BBL 2020 233.

registered office or, if there is no such office, its habitual residence, shall apply. With respect to proprietary interests in physical titles, reference is made to Chapter 7 on international property law.

3.1.3 Germany

In 2021, Germany passed the Electronic Securities Act (eWpG),[25] which is restricted to electronic bearer bonds and similar investment tools but may serve as a model for other types of securities. It introduces the possibility of creating electronic securities by way of a book-entry in either a central register (to be maintained by central securities depositories or another custodian, provided that the issuer expressly authorises the custodian to do so) or a crypto securities register (to be maintained on a tamper-proof ledger by the issuer or an entity designated as such by the issuer).

Section 32(1) of the eWpG provides that the conflict rules in Section 17a of the Custody Act (DepotG) for intermediated securities take priority within their scope of application. This concerns cases where the DepotG is applicable because electronic securities are held in collective custody, *i.e.*, as a rule in the case of electronic securities held in collective custody based on collective entry as well as in the case of electronic securities which are registered in collective entry and which are booked by the depositary in a deposit account of the depositor pursuant to Section 9b(1) of the DepotG.[26] Where these rules do not apply, *e.g.*, because the electronic securities are not held through an intermediary, rights in an electronic security and transfers of electronic securities or the granting of rights in rem are governed by the law of the state under whose supervision the relevant register-keeping body operates. If the entity keeping the register is not subject to supervision, the seat of the entity keeping the register shall be taken as a connecting factor, and failing that, the registered office of the issuer.

3.1.4 United States

In the United States, conflict of laws, including with regard to digital assets, is largely state law. It was only recently that the Uniform Commercial Code Amendments 2022 were published, after having been drafted by the Uniform Law Commission (ULC) in partnership with the American Law Institute (ALI). They were approved and recommended for enactment in all the states

25 2021 Electronic Securities Act (Gesetz über elektronische Wertpapiere vom 3. Juni 2021; "eWpG").

26 Report of the Financial Committee of the German Federal Parliament, BT-Drucksache 19/29372, 5 May 2021, 58.

at the ULC meeting in Philadelphia in July 2022, after they had already been approved by the ALI Membership in May 2022. The new Article 12 contains several Sections on governing law with regard to digital assets as far as they qualify as 'controllable electronic records' within the meaning of the new UCC provisions. Section 12–107, in particular, determines a controllable electronic record's jurisdiction.

In the first place, the UCC follows the principle of elective situs: if the controllable electronic record, or a record attached to or logically associated with the controllable electronic record and readily available for review, expressly provides that a particular jurisdiction is the controllable electronic record's jurisdiction, the law of that jurisdiction applies. Where there is no such express provision at the level of the controllable electronic record (*e.g.* a particular class of tokens) itself, but where the rules of the system in which the controllable electronic record is recorded (*e.g.* the Ethereum blockchain) are readily available for review and expressly provide that a particular jurisdiction is the controllable electronic record's jurisdiction, the law of that jurisdiction applies. In either case, an express provision that makes reference to Article 12 UCC takes precedence over a more general provision. If no such provision exists the controllable electronic record's jurisdiction is the District of Columbia.

3.2 *Proposed Legislation and Soft Law*

Given the novelty of crypto assets as a phenomenon, many countries and regions as well as international organisations are still in the phase of preparing legislation, model rules and principles to guide legislators worldwide, or draft international conventions.

3.2.1 The Proposed EU Regulation on Third Party Effects of Assignments of Claims

In 2018, the European Commission published a Proposal for an EU Regulation on the law applicable to the third-party effects of assignments of claims (TPE Regulation).[27] The original proposal does not mention crypto assets at all, but only claims in general. However, this has changed in the course of legislative work, in particular work by the Council working group. The latest document is a Council document dated 3 December 2021, displaying a 4-column table for the Regulation as resulting from the initial positions of the three EU institutions.[28]

27 Proposal for a Regulation of the European Parliament and of the Council on the law applicable to the third-party effects of assignments of claims, [2018] COM/2018/096 final ("TPE Regulation").

28 Council of the European Union, "Proposal for a Regulation of the European Parliament and of the Council on the law applicable to the third-party effects of assignments of

The proposed TPE Regulation will most likely not apply to the third-party effects of the transfer of crypto assets, whether or not they qualify as financial instruments, including by way of security, pledges or other security rights over such crypto assets,[29] like it will not apply to the third-party effects of the transfer of financial instruments, including by way of security. However, while claims incorporated in a certificate or represented by a book-entry, as well as claims arising out of a transferable security, will probably be excluded from the scope altogether, claims arising from other financial instruments and from crypto assets are currently proposed by the Council to be included. However, they enjoy special treatment. While the default rule for claims is that third-party effects of an assignment shall be governed by the law of the State in which the assignor has its habitual residence at the material time of the conclusion of the assignment contract,[30] the third-party effects of the assignment of cash claims and electronic money claims, as well as claims arising out of, inter alia, financial instruments and crypto assets, shall be governed by the law applicable to the assigned claim.

As the TPE Regulation will not apply to the transfer of crypto assets as such, its significance for the law applicable to proprietary rights in crypto assets will be limited, but the fact that third party effects of the assignment of claims arising from crypto assets will most likely be subjected to the law governing the assigned claim, this may be an argument for considering this law also for the proprietary rights in the underlying assets themselves.

3.2.2 ELI Principles on the Use of Digital Assets as Security

In early 2022, the European Law Institute (ELI) published the 'ELI Principles on the Use of Digital Assets as Security'.[31] These address only security interests such as a pledge, but, as it would be difficult to apply a different law to transfers of title (considering, in particular, that full title may be transferred also for security interest purposes), the views expressed by its authors are relevant for proprietary interests in digital assets in general. The Principles start by clarifying that they are without prejudice to the treatment of digital assets already regulated as financial instruments under national law and, where applicable, EU or other supranational law. The Comments elaborate that the Principles do not apply at all, inter alia, to financial instruments within the meaning of Article 4(1)(15) of the Second Markets in Financial Instruments Directive

---

claims – 4 column table" (*EC*, 3 December 2021) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_14544_2021_INIT&from=EN>.

29 TPE Regulation (n 27), Proposed Article 1 (1ab).

30 *Id*. at Proposed Article 4.

31 See above at (n 5).

(MiFID II)[32] and to electronic money within the meaning of Article 2(2) of the Second E-Money Directive[33] (unless tokenised).[34] This is in order not to interfere, in particular, with the Financial Collateral Directive (FCD)[35] and the Settlement Finality Directive (SFD).[36]

The Principles designate primarily the law of the jurisdiction in which the security provider has, at the time of the creation or perfection of the security interest, its place of business, or its central administration (if it has a place of business in more than one jurisdiction) or the law of the jurisdiction in which the security provider has its habitual residence as the law applicable to both creation and perfection of a security interest. However, this is not the case where the digital asset itself is clearly connected with one particular jurisdiction, in which case the law of that jurisdiction is to be the applicable law. The Comments give the example of a permissioned DLT system, established by an identifiable issuer in an identifiable jurisdiction, operating subject to the laws of that jurisdiction and intended to operate within a single legal system which is known to all permissioned participants. By contrast, the general rule of the place of the security provider should, according to the Comments, prevail for digital assets held through a custodian or another intermediary, as the law of such custodian or intermediary could also be relevant in designating the law that is most closely connected with a security arrangement.

3.2.3 UNIDROIT Work in the Field

As part of 2020–2022 Triennial Work Programme, a Working Group of the International Institute for the Unification of Private Law (UNIDROIT) has been

32 Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU, [2014] OJ L173/349 (Second Markets in Financial Instruments Directive; "MiFID II").

33 Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC, [2009] OJ L267/7 ("E-Money Directive").

34 *Id*. at Principle 1(4). A range of further types of assets has been excluded, mirroring exclusions from the scope of application of the MiCA Proposal. It is not clear, though, why this has been done as the relevant EU law focuses on supervisory matters.

35 Directive 2002/47/EC of the European Parliament and of the Council of 6 June 2002 on financial collateral arrangements, [2002] OJ L168/43 (Financial Collateral Directive; "FCD").

36 Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems, [1998] OJ L166/45 (Settlement Finality Directive; "SFD").

established with the objective to develop a future legal instrument containing principles and legislative guidance in the area of private law and digital assets. The preparation of a guidance document is expected to be adopted in 2023.

The UNIDROIT Working Group (Working Group on Digital Assets and Private Law – DAPL WG) had pursued, from the beginning, an approach according to which the law applicable to propriety questions in respect of digital assets should be identical for all digital assets of the same description. This is significantly different as compared with the ELI Principles, which favour the location of the security provider, thereby accepting that very different laws apply regarding digital assets of the same description. The UNIDROIT drafts then continue by setting out a waterfall of connecting factors, referring to the law chosen at the moment of the first issuance of assets being of a specific description, and, failing that, the law generally chosen for the network/system on which the relevant digital assets are created. On the question of what should be the third step of the waterfall, there have been remarkable changes during the work of the Working Group. Study LXXXII - W.G.5 - Doc. 3 of February 2022 still referred to the law of the State with which the network/system has the strongest factual connection, in particular through any location of the network operator. Following the adoption of the new Article 12 UCC by both the ALI and the ULC, the UNIDROIT Working Group, in its subsequent Working Group meetings, clearly sought to align Principle 5 with the solutions now favoured by U.S. law by referring, at the third step of the waterfall, to the Principles themselves. However, the negotiations during the 8th session of the Working Group in March 2023 seem to have reversed this course, with the latest version of the conflict-of-laws provision showing much less U.S. influence and a more nuanced approach.

Principle 5 of Study LXXXII - W.G.8 - Doc. 6, dated March 2023,[37] determines the law applicable to property issues in relation to a digital asset to be primarily the domestic law of the State, or these Principles, or the relevant Principles or aspects of these Principles governing property issues, expressly identified in the digital asset as the law applicable to such issues. Where this is not the case, reference will be made to the national law of the State which is expressly identified in the system or platform on which the digital asset is recorded as the law applicable to such matters. At the third step of the waterfall, there is now a reference to the issuer, which is defined as the legal entity that has placed the digital asset into the stream of commerce for value. There are still several

37 See UNIDROIT Study LXXXII - W.G.8 – Doc. 6 <https://www.unidroit.org/wp-content/uploads/2023/03/W.G.8-Doc.-6-Tracked-and-Updated-Principle-5.pdf> accessed 15 March 2023.

options at the bottom of the waterfall, all of which give a state considerable freedom to choose the appropriate rules for a forum located in that state. The current design of the UNIDROIT conflict-of-law rule is therefore a combination of the US model and the Swiss approach, although other influences are also evident. According to its mandate, the DAPL WG aims to finalise the draft UNIDROIT Principles in 2023.[38]

3.2.4 HCCH Work in the Field

The Hague Conference has been considering starting work on private international law aspects of digital assets for some time. At its 2020 meeting, the Council on General Affairs and Policy (CGAP) invited the Permanent Bureau (PB) to monitor developments.[39] At the 2021 CGAP meeting, the PB invited CGAP to consider creating an Experts' Group to assess the desirability, necessity and feasibility of a new instrument on jurisdiction, applicable law, recognition and enforcement in respect of digital assets.[40] The Preliminary Document No. 4 of November 2020, which was discussed at the 2021 CGAP meeting, includes a table with no less than 12 alternative connecting factors for determining the law applicable to proprietary rights in digital assets which lists the benefits and downsides of each solution without indicating a clear preference. The document relies heavily on a study conducted in 2018 by the UK Financial Markets Law Committee, which listed an equal number of connecting factors without a clear conclusion.[41] At the 2022 CGAP meeting, an extended report on current developments was submitted,[42] and the 2023 CGAP meeting revealed that the HCCH will closely cooperate with UNIDROIT in the field as the PB and the UNIDROIT Secretariat have discussed continued cooperative work on a joint project focused on digital assets and tokens ("HCCH-UNIDROIT Digital Assets and Tokens Project").[43] The project would, broadly, build on and expand the work that has been carried out by the DAPL WG, in particular Principle 5 of the draft UNIDROIT Principles.

---

38 UNIDROIT Governing Council, Summary Conclusions 101st session C.D. (101) Misc. 2 rev (June 2022), no. 26.

39 HCCH, "Proposal for the Allocation of Resources to Follow Private International Law Implications relating to Developments in the Field of Distributed Ledger Technology, in particular in relation to Financial Technology," Prel. Doc. 28 February 2020, para. 19.

40 HCCH, "Developments with respect to PIL implications of the digital economy, including DLT," Prel. Doc. No 4 of November 2020, para. 30.

41 Financial Markets Law Committee (n 18), 15 *et seq*.

42 HCCH, "Developments with respect to PIL Implications of the Digital Economy," Prel. Doc. No 4 REV of January 2022.

43 HCCH, "Proposal for Joint Work: HCCH-UNIDROIT Project on Law Applicable to Cross-Border Holdings and Transfers of Digital Assets and Tokens," Prel. Doc. No 3C of January 2023, para 16 *et seq*.

4 Use of DLT for Traditional Classes of Assets

Due to the broad variety of digital assets, including crypto assets, it may be difficult to formulate one single set of conflict-of-laws rules, and different classes of assets may require differential treatment. To start with, DLT may be used to complete transactions in very traditional classes of assets.

4.1 *Central Bank Digital Currencies* (*CBDC*)

Central banks can, in principle, issue currencies that are legal tender in whatever form. Historically, central bank currencies have been coins and banknotes, with additional money being created by commercial banks handing out loans and lending money from the central bank. Theoretically, a central bank can decide to no longer mint metal coins and print paper banknotes, but to issue digital coins instead and give them the same status as cash has today. For CBDC to become legal tender, existing legislation usually needs to be amended, stating, or at least clarifying, that CBDC have the same status as cash. Ideally, this legislation would then also clarify whether units of the CBDC are to be treated analogously to tangible property or in some different manner, or even include an explicit conflict-of-laws rule.

For CBDC that replace physical coins and banknotes, there are, in principle, two alternative connecting factors: (i) the seat of the issuing central bank; or (ii) the place of the relevant holder, with the usual uncertainties as to how this place is to be determined (*e.g.*, whether it is physical presence that counts, or residence, habitual residence, domicile, central administration, relevant branch office *etc.*). Alternatively, CBDC could be submitted to the same conflict-of-law rules as other crypto assets.[44]

At a closer look, it seems to be preferable to go for the first solution, *i.e.*, to apply the law of the state where the issuing central bank has its seat. This seat will not only be much easier to determine than the place of the current holder (not to mention the possibility of joint holders in different countries) and be much more stable, but the law of that state will naturally also include legislation about the CBDC in general, including on the conditions under which the CBDC is issued, whether it is to be treated analogously to cash under a legal fiction or in some different manner and other details. It would be unfortunate to risk a clash between any provisions in such legislation and another law applicable to proprietary rights in CBDC. Therefore, proprietary rights in CBDC should be governed by the law of the state where the issuing central bank has its seat.

---

44 HCCH, "Developments with respect to PIL Implications of the Digital Economy," Prel. Doc. No 4 REV of January 2022, para 29 et seqq; HCCH, "Proposal for Exploratory Work: Private International Law Aspects of Central Bank Digital Currencies (CBDCs)," Prel. Doc. No 3B of January 2023, para 3 *et seq*.

4.2 *Tokens Qualifying as Electronic Money*

Furthermore, credit institutions and other institutions are authorised to issue electronic money under the legal provisions implementing the E-Money Directive and can, in principle, do so in any appropriate electronic form. For instance, it would be admissible to have the e-money stored on a magnetic strip or chip embedded in a prepaid card, or within software on a terminal device, but there is nothing that would prohibit issuing electronic money with the help of DLT. Therefore, tokens may already today directly qualify as e-money given that they entail a claim of the holder against the issuer.

However, there exist also crypto assets referencing a single fiat currency but failing to provide their holders a contractual right to redeem their electronic money at any moment against fiat currency that is legal tender at par value with that currency. To avoid circumvention of the rules laid down in the E-Money Directive, the MiCA Proposal now suggests extending the strict provisions that apply to the issuers of e-money to the issuers of crypto assets referencing a single fiat currency ('e-money tokens'), so such tokens would, in the future, be subject both to the E-Money Directive and the proposed MiCA Regulation.

Neither the E-Money Directive nor the proposed MiCA Regulation include any provisions on applicable law. Again, there is basically the choice between (i) the seat of the issuer of the e-money, or rather the state under whose supervision the issuer of the e-money operates, and (ii) the place of the current holder of the e-money. Whereas the state under whose supervision the issuer operates (and which will normally coincide with the seat of the issuer) may not be as obvious and as stable as that of a central bank, there may still be convincing reasons to go for the law of that state rather than for the law at the place of the current holder: given that the law of the relevant supervisory authorities will normally also define the conditions under which e-money may be issued, redeemed against fiat currency, *etc.*, it would be unfortunate to risk a clash between that law and any other law deciding about proprietary rights in e-money.

4.3 *Tokens Qualifying as Financial Instruments*

Finally, there is nothing to stop a legislator from introducing financial instruments, in particular securities, in electronic form and/or on DLT. Nowadays, much of the market in financial instruments is electronic anyway, with a book entry in an account replacing possession of the physical certificate.

4.3.1 Traditional Rules for Intermediated Securities

Even though certified (paper) securities are a phenomenon of the past, some countries, such as Austria or Germany, have been clinging to a 'quasi-physical

fiction' until today[45] with holders becoming co-owners of a fraction of a global certificate held in collective safe custody. The holder's co-ownership share in the securities portfolio is evidenced by the account statement of the holder's commercial bank. The actual custody and administration of securities from domestic issuers takes place at the relevant Central Securities Depository (CSD). Securities from foreign issuers are held in safe custody with a foreign central administrator, which maintains mutual account details with the domestic CSD. When Germany introduced 'electronic securities' to be registered either in a central register or in a crypto securities register (see above at 3.1.3), the 'quasi-physical fiction' was upheld, *i.e.*, even electronic securities are treated analogously to tangible property under German law. Other countries, such as Switzerland, have long taken the step to introduce fully 'paperless' securities, with registration in a securities registry required in lieu of issuance of individual or global certificates, with transfer occurring by way of assignment.[46] There are also many countries adhering to the securities entitlement system, such as the U.S.,[47] whereby the holder normally has rights only against the next intermediary with whom the holder has an account.

Tokens which directly qualify as financial instruments, in particular securities, should also be treated like financial instruments for conflict-of-laws purposes. This means for EU Member States that provisions implementing Article 9(1) of the FCD and Article 9(2) of the SFD apply in the first place. Although they have a somewhat limited scope of application, it is arguably not advisable to restrict the conflict rules expressed therein to that narrow scope, but instead to take them as the basis for a more general principle designating the law applicable to intermediated financial instruments. Reference is made to 'the law of the country in which the relevant account is maintained' and to the law of the Member State in which the 'register, account or centralised deposit system' is located in which security rights are 'legally recorded'. The applicable law is therefore more generally the law of the state of the account where the right in question is recorded, which, in the case of intermediated securities, is the security provider's account in the case of a pledge or similar security right, and the transferee's account in the case of a full transfer of title.[48]

45 Cf. Austrian Securities Deposit Act (*Depotgesetz*), section 5; German Safe Custody Act (*Depotgesetz*), section 6.

46 Matthias Lehmann, *Finanzinstrumente* (Mohr Siebeck 2009), 83 *et seq*.

47 See Part 5 of the Uniform Commercial Code (UCC).

48 Wendehorst, "Art. 43 EGBGB," (n 1), n. 233, 243 *et seq*.

For the Contracting States applying the 2006 Hague Securities Convention,[49] the conflict rules provided by that Convention will apply instead. However, the question arises what this may mean for digital assets.

4.3.2 When Do Intermediated Digital Assets Qualify as Intermediated Securities?

Digital assets held by an intermediary may fall under the rules for intermediated securities, and if they do, the conflict rules derived from the FCD and SFD or the 2006 Hague Securities Convention will take priority. Looking at the wording of the relevant provisions, there is not much guidance concerning the types of custody covered. However, it is also clear that the relevant rules have been drafted with the centralistic and highly regulated system of clearing and settlement mechanisms in mind, which exists regarding transferable securities in current accounts and where a book-entry may trigger immediate proprietary or quasi-proprietary effects.

Originally, reducing reliance on intermediaries was one of the main reasons for parties to use DLT, as DLT may allow participants in a peer-to-peer network to hold and transfer assets without any additional service providers. In reality, though, this is hardly ever the case. Rather, a very diverse ecosystem of different service providers has come into existence. The MiCA Proposal already lists eight different types of 'crypto-asset services': the custody and administration of crypto assets on behalf of third parties, the operation of a trading platform for crypto assets, the exchange of crypto assets for fiat currency that is legal tender, the exchange of crypto assets for other crypto assets, the execution of orders for crypto assets on behalf of third parties, the placing of crypto assets, the reception and transmission of orders for crypto assets on behalf of third parties and providing advice on crypto assets. The service that is most akin to the service provided by intermediaries which the drafters of the FCD, SFD or the 2006 Hague Securities Convention had in mind is the custody and administration of crypto assets on behalf of third parties, *i.e.*, a type of service normally provided by wallet providers and crypto exchanges.

Where crypto assets directly qualify as securities or other financial instruments, and where a provider of custody services actually holds the crypto assets in a register of positions, opened in the name of each client, corresponding to each client's rights to the crypto assets, it will at first sight be difficult to argue why the existing conflict rules for intermediated securities

49 HCCH, "36: Convention of 5 July 2006 on the Law Applicable to Certain Rights in Respect of Securities held with an Intermediary" (*HCCH*, 2016) <www.hcch.net/index_en.php?act=conventions.text&cid=72> accessed 15 March 2023.

should not apply. At a closer look, a major difference seems to be that the register in which the entry triggering proprietary or quasi-proprietary effects is made is not the account opened for the individual client, but the distributed ledger on which the relevant crypto asset exists. In other words: where Alice transfers traditional book-entry securities to Bob, Bob will hold a proprietary or quasi-proprietary right in the book-entry securities once they have been booked to his account, with an intermediary taking part in the relevant clearing and settlement system. However, where Alice transfers to Bob crypto assets via a crypto-assets service provider, what counts is whether Bob's custody provider has actually acquired the assets for Bob on the distributed ledger on which they exist. So, the relevant book-entry with proprietary effects is in the distributed ledger, not in the register of positions held with the intermediary.

At the end of the day, this difference may be relevant for the EU approach, which still relies on the actual 'location' (in terms of state supervision or seat) of the relevant register or account in which the proprietary or quasi-proprietary effects are triggered. Countries adhering to this approach will apply PRIMA only where the effect of a book-entry with regard to electronic securities is comparable to the effects of a book-entry with traditional securities. However, for countries that have largely given up the idea of actual 'location' of a register or account, including countries following the Hague Convention approach of relying on the law chosen by the parties to the account agreement (with certain limitations to choice), the difference will be less relevant. So, at least for those countries, the conflict rules applied for intermediated securities may already be applicable to DLT-based securities.

5 The Law Applicable to Proprietary Interests in Tokens beyond Existing Conflict Rules

This leaves a gap for digital assets that either (i) do not qualify as securities or other financial instruments and therefore do not fall under any of the recognised conflict rules (*e.g.*, bitcoin, stablecoins, utility tokens or NFTS); or that (ii) qualify as securities or other financial instruments within the meaning of financial markets law, but for which existing conflict rules do not fit. The latter may be the case, *e.g.*, where a legal system has rules only for intermediated securities, but the securities in question are not held through an intermediary, or the relevant conflict rules for intermediated securities do not fit the situation with DLT and the legal system has not yet created a fall-back regime, such as Germany has created with Section 32 of the eWpG.

5.1 *Special Conflict Rules for Exogenous Tokens?*

In a first step, the question arises whether proprietary rights in exogenous tokens (see above at 2.2) are potentially governed by a different law than the law governing proprietary rights in the represented asset, or whether the former is always identical with the latter.

5.1.1 The Law Governing the Effects of Tokenisation as Such

At a closer look, the question falls into two parts, the first being that of the link between the digital asset and the represented asset. If, for example, the ownership of a painting is 'tokenised' the question arises whether and, if so, under what conditions the transfer of the token to another participant in the network also transfers ownership of the painting. By and large, this must be decided by the law governing proprietary rights in the represented asset,[50] *i.e.*, in the example of the painting, usually the place where the painting is located (according to the *lex situs rule*, which is almost universally recognised), in the case of claims, the law governing the claim (according to Article 14 (2) Rome I Regulation[51]) and in the case of company shares, the law governing the company, *etc*.

Ideally, the law governing proprietary rights in the represented asset will fully clarify the relationship with the digital asset. The Liechtenstein Law on Tokens and Trusted Technology Service Providers (TVTG) can be cited as an example. Article 7(1) of the TVTG states that the transfer of the token has the effect of the transfer of the right vested in the token. However, if the legal effect does not occur by operation of law – for example, because registration is required – the transferor must ensure by appropriate measures that the transfer of the token directly or indirectly leads to the transfer of the right represented, and the represented right cannot be transferred to a different person in the meantime. Furthermore, pursuant to Article 8 of the TVTG, the person entitled to transfer the token as identified by the system shall be deemed to be the lawful owner of the right represented in the token vis-à-vis a third-party debtor, and the debtor shall be discharged by payment to the person designated by the system as the owner of the token, unless the debtor knew or should have known that the designated owner is not the lawful creditor.

Where the law governing proprietary rights in the represented asset does not recognise the proprietary effects which the parties tried to achieve through tokenisation, there is still the possibility that a consensual transaction in the booking system can be construed as an exchange of at least implied declarations of intent which, according to the rules applicable outside the booking system, can nevertheless bring about legal effects. This will often be the case,

50 Wendehorst, "Art. 43 EGBGB," (n 1), n. 200.

51 See now, however, the TPE Regulation (n 27).

for example, with assignments of claims and other intangibles, but also potentially with tangible property if the law applicable to proprietary rights follows the consensus principle. Even where this is not the case, the transaction on the ledger may produce a contractual obligation to transfer the represented right outside the ledger by conventional means.

5.1.2 The Law Governing Proprietary Rights in the Digital Asset

While it is not very controversial that the law governing proprietary interests in the represented asset must decide about the effects of tokenisation, including about the effects a transfer of the digital asset has on the represented asset, it is not clear whether the third-party effects of a transfer of the digital asset are governed by the same law or by a different law.

Obviously, having proprietary interests in the token be governed by the same law that is already governing proprietary interests in the represented asset would have a range of advantages. There would be a clear connecting factor, and clashes between possibly diverging results achieved by the one law or by the other would be avoided. For instance, if the token represents ownership in a (physical) painting and the *lex situs* with regard to the painting would not allow a *bona fide* purchase where the purchaser buys from a thief, it would be consistent not to allow a *bona fide* purchase of the token where the private key had been stolen from the legitimate holder. On the other hand, this would also mean that where the painting is moved across borders to the territory of a State whose law does allow a *bona fide* purchase in this situation, the same would apply for the token, *i.e.*, the law applicable to proprietary interests in the token would change as the law applicable to proprietary interests in the represented asset changes. This would be inconsistent with the desire for certainty and security which the parties to a token transaction usually have and which is the main motivation for tokenisation.

Interestingly, among the many different options discussed in legal literature and by UNIDROIT (see above at 3.2.3) and HCCH (see above at 3.2.4), having the law governing proprietary interests in the represented asset automatically govern proprietary rights in the token does not seem to be very popular either. At the end of the day, it seems that the law governing proprietary rights in the digital asset should not automatically coincide with the law governing proprietary rights in the represented asset.

5.2 *Connecting Factors Focusing on the Parties Involved*

By and large, two different types of connecting factors exist: connecting factors focusing on the parties involved in a transaction and connecting factors focusing on the asset itself. The former can be divided into connecting factors focusing on the location of the holder or transferor and connecting factors focusing on an intermediary or account.

In the law of obligations, the applicable law is usually determined by connecting factors that have something to do with the parties, be it a choice of law by the parties, the parties' habitual residence or the place where some activity of a party occurred. As far as proprietary aspects are concerned, and at least where the legitimate interests of third parties come into play, this kind of connecting factor is less common. The habitual residence of the assignor is now being proposed as a default rule in the draft EU Regulation on Third-Party Effects of Assignments of Claims (see above 3.2.1), but not for electronic money claims or claims arising from financial instruments or crypto assets. A similar rule has been proposed by the UNCITRAL Model Rules on Secured Transactions,[52] but generally as a default rule with regard to intangible assets, with many exceptions for particular types of intangible assets and without having considered the specificities of crypto assets at the time. The only major instrument that seems to be proposing the place of the security provider as a connecting factor specifically for digital assets is the ELI Principles on the Use of Digital Assets as Security (above at 3.2.2).

A very different group of party-focused connecting factors are used by the many variants of the PRIMA (*Place of the Relevant InterMediary Approach*) principle, including its modification by the Hague Securities Convention, which is better characterised as AAA (*Account Agreement Approach*). These connecting factors are not focused on the parties to a transaction, but on the intermediary or the account agreement, chosen by one of the parties to a transaction, be it the transferor (security provider) or transferee (security taker). As has been explained in more detail above (see at 4.3.2), the type of intermediaries we find in the context of crypto assets (custody providers) are not fully comparable to the type of intermediaries we see in the context of intermediated securities, as the book-entry that triggers proprietary or quasi-proprietary effects does not occur in the account which the individual holder has with its intermediary but in the distributed ledger. Interestingly, the approach is hardly being discussed in the context of crypto assets, except under the heading of 'location of private user key'.[53]

5.3 *Connecting Factors Focusing on the Digital Assets*

Another group of connecting factors focuses on the digital assets themselves, trying to achieve uniformity of solutions within the same type of digital assets, such as a particular type of tokens issued by a particular issuer. This is an

52 UNCITRAL, "UNCITRAL Model Law on Secured Transactions (2016)" (*UNCITRAL*, 2016) <https://uncitral.un.org/en/texts/securityinterests/modellaw/secured_transactions> accessed 15 March 2023.

53 Financial Markets Law Committee (n 18), 18.

objective stressed, in particular, by the UNIDROIT work in the field (see above at 3.2.3). Such connecting factors would normally be associated with a public register, with the issuer, with the network operator or with another person (different from the parties to a transaction) that has something to do with the digital assets.

5.3.1 Lex Libri Siti

Where digital assets require, by virtue of public law, an entry in a public register, the place of that register is an obvious connecting factor. The 'place' cannot mean the location of the relevant servers, though, as server location is hardly an appropriate and reliable criterion. Rather, the place of a register is primarily the state under whose supervision the register is maintained, *i.e.*, to whose regulation the entity maintaining the register submits its activities, and if the entity maintaining the register is not under supervision, the state where that entity has its seat.[54]

5.3.2 Elective Situs

Another possible connecting factor is choice of law by the issuer (*i.e.*, at the level of the class of digital assets, such as tokens resulting from one and the same ICO), or by the system administrator (*i.e.*, at the level of the DLT network) in a way that is visible to all relevant participants, so that any person participating in the system can be deemed to have accepted the choice (*'elective situs'*).[55] The arguments otherwise put forward against the choice of the applicable law in international property law would not apply, provided that this choice of law is recognisable to any third party at first glance. Of course, there remain concerns that the interests of certain parties could be harmed by the choice of the most liberal law possible, which is why one could also consider restricting available legal systems to those that have some minimum contacts with the issuer or the system administrator.[56]

Where digital assets are subject to registration under a particular legal system, there are strong arguments for deeming the issuer to have chosen the law of the relevant state. In any case, the choice of law would neither affect supervisory law nor investor protection law, but only property law.

---

54 Wendehorst, "Art. 43 EGBGB," (n 1), n. 212; Michael Born, *Europäisches Kollisionsrecht des Effektengiros* (Mohr Siebeck 2014), 71.

55 Financial Markets Law Committee (n 18), 15 *et seq.*; Michael Ng, "Choice of law for property issues regarding Bitcoin under English law," (2019) 15 Journal of Private International Law 315, 332; cf. on the whole also Felix Krysa and Matthias Lehmann, "Blockchain, Smart Contracts und Token aus der Sicht des (Internationalen) Privatrechts," (2019) 2 Bonner Rechtsjournal 91 *et seq*.

56 Financial Markets Law Committee (n 18), 16.

5.3.3 LIMA

If the issuer of a digital asset is known and its seat is sufficiently clearly recognisable for third parties, the seat of the producer or issuer seems to lend itself (*Location of the Issuer Master Account*; *'LIMA' principle*).[57] According to the TVTG of Liechtenstein, tokens are also considered domestic assets if they are created or issued by a provider of so-called 'trusted technologies' (VT service provider) domiciled in Liechtenstein. However, a link to the seat of the issuer requires that its identity and domicile are clearly recognisable to third parties, which is not necessarily the case, particularly with cryptocurrencies (which often do not have an identified issuer), but also with many tokens.

5.3.4 PROPA and PREMA

As an alternative to LIMA – especially if a creator or issuer in the narrower sense does not exist or its registered office is not precisely known – it is also possible to focus on the location of another central authority, if such an authority exists.[58] This can be a state authority or a body (*e.g.*, a foundation) that takes over the administration of the system (*Place of the Relevant OPerating Authority/Administrator; 'PROPA' principle*). The seat of a body that holds a system-relevant master key, with the help of which coercive transactions can be carried out, for example, based on a court order (*Primary Residence of the Private Encryption MAster key-holder*; *'PREMA' principle*), can also be considered. However, the PREMA principle leads to problems if several authorities hold a master key.[59]

5.3.5 Other

Other connecting factors mentioned, such as the residence of the programmer (*Primary Residence of the Coder*; *'PResC' principle*),[60] seem to be rather far-fetched. Be that as it may, it is clear that, for many types of assets – such as bitcoin – almost all attempts to establish a clear connection with a particular state will lead to less than satisfactory results. However, from the beginning, there will always be some entity connected in some meaningful way with a cryptocurrency. Scholars have proposed, for example, to seek a connection

57 Frank Schäfer and Thomas Eckhold, in Heinz-Dieter Assmann, Rolf A. Schütze and Petra Buck-Heeb (eds), *Handbuch des Kapitalanlagerechts*, (5th edn, C.H. Beck 2020), § 16a n. 49, assuming this as the only possible connection.

58 Financial Markets Law Committee (n 18), 18 *et seq.*; Dieter Martiny, "Virtuelle Währungen, insbesondere Bitcoins, im Internationalen Privat- und Zivilverfahrensrecht," (2018) 6 Praxis des Internationalen Privat- und Verfahrensrechts 553, 559.

59 Christiane Wendehorst, "Digitalgüter im Internationalen Privatrecht," (2020) 6 Praxis des Internationalen Privat- und Verfahrensrechts 490, 497.

60 Ng, (n 55), 334; Financial Markets Law Committee (n 18), 22.

to the law of the US state of Massachusetts as a way out for the Bitcoin blockchain.[61]

5.4 *Discussion*

Arguments put forward by the ELI Principles in favour of having proprietary rights in crypto assets governed by the place of the transferor (security providers, *etc*.) are: that the rule is straightforward in its application and does not require any complicated classification of digital assets, that it is relatively stable and transparent *vis-à-vis* security takers, that it offers a point of reference for deciding on the relative priority of competing claims, that it would in most cases coincide with the relevant insolvency law and that it would facilitate bulk transfers, thus serving the interests of the takers of security in heterogeneous portfolios of assets.[62]

Arguments put forward against this rule are: that it requires a complicated mechanism for determining priority of security interests, poses problems in cases of joint transferors, chains of assignments or change of habitual residence, that the rule artificially splits up the DLT record and may harm the interests of third parties for whom it may be difficult or impossible, in particular in a pseudonymised DLT environment, to determine the habitual residence of a participant at a given point in time.[63] Also, it would not coincide with law applicable to claims arising from crypto assets under the proposed TPE Regulation, nor would it coincide with the law applicable to intermediated securities.

Conversely, the advantage of connecting factors that focus on the digital assets themselves is that proprietary rights in one and the same identified asset, as well as in one and the same class of assets, will be governed by one law, which greatly helps with chains of assignment and determining priority of competing claims. These connecting factors are also immune against changes in habitual residence, changes of custody service provider and problems of joint ownership. Provided the law applicable regarding the same class of digital assets is sufficiently visible to third parties, this guarantees the kind of certainty required regarding proprietary aspects. Also, given that claims arising from crypto assets will most likely be governed by the same law as the crypto assets themselves, a connecting factor focusing on the crypto assets would more likely coincide with the law designated by the proposed TPE Regulation for claims.

Not surprisingly, the downside is that bulk transactions (such as the creation and perfection of security interests in heterogeneous portfolios of assets) are made more complicated, as each type of asset included in the portfolio

61 Ng, (n 55), 336 *et seq*.

62 European Law Institute (n 5), 27

63 HCCH (n 49), 10.

would potentially be governed by a different law. Conflict rules would take the form of rather complicated waterfalls, and waterfalls may be different from country to country.

6 Summary

The law governing rights with third party effect (proprietary rights, rights in rem) in digital assets has been a point of controversy for some time, particularly regarding crypto assets. Part of the problem stems from the fact that crypto assets exist on distributed ledgers and therefore cannot be 'located' in the way tangible assets can, but that they cannot readily be qualified as 'rights', either.

Theoretically, a similar phenomenon has existed for a long time with book-entry securities, which are also intangible but at the same time distinct from any underlying shares or claims and designed to facilitate the latter's circulation. There is no unanimous view globally as to how proprietary rights in book-entry securities should be dealt with under the conflict of laws, but most approaches would try to 'locate' the relevant book-entry that records the proprietary right in question. There are different methods of 'locating' book-entries, such as by reference to the place of the intermediary maintaining the relevant account (PRIMA), to the law designated to govern the relevant account agreement (AAA) or combinations thereof. As the world is seeing a convergence between certified, book-entry and electronic securities, as well as between cash, bank and cryptocurrencies, analogies may be drawn. However, this must be done with caution, *e.g.*, while there exists a rather clear notion of what counts as an 'intermediary' in the context of intermediated securities, this is much less clear in the case of crypto assets.

By and large, two main opposing views seem to exist. The one, taken by the ELI Principles on the Use of Digital Assets as Security, takes the location of the holder (transferor, security provider) as the connecting factor for all crypto assets that are not already subject to existing conflict rules. The advantage of this rule is its simplicity and uniformity, as well as the legal certainty it provides for bulk transactions where the identity of the transferor is known to the transferee. Its downsides are complications in the context of chains of assignments, joint holders and changes of location, and it fails altogether in contexts where the identity and location of the holder is unknown. The other approach, which seems to be the prevailing view so far, seeks to achieve uniformity of results within one and the same class of assets, such as coins generated in the course of one and the same issue, trying to 'locate' a particular crypto asset in

accordance with a choice of law (elective situs) or some objective criterion (such as the seat of the issuer), usually ending up with a waterfall of connecting factors or several different waterfalls. With crypto assets such as bitcoin, any convincing 'location' will normally fail, so there needs to be a solution for the bottom of the waterfall.

With the imminent adoption and publication of UNIDROIT's work on Digital Assets and Private Law, in particular its Principle 5, a major step forward will be taken. Broadly speaking, it introduces a waterfall that starts with choice of law made for digital assets of the same description, failing that choice of law made for the relevant network or system. The waterfall continues with the seat of the issuer and ends with a range of solutions close to a lex fori principle. As HCCH and UNIDROIT have now jointly announced to start a "HCCH-UNIDROIT Digital Assets and Tokens Project", more clarity is to be expected soon: there is thus light at the end of the tunnel.

CHAPTER 6

The Good, the Bad and the Ugly: The Private International Law, the Crypto Transactions and the Pseudonyms

Anne-Grace Kleczewski

1 Introduction

Presently, Private International Law (PIL) is under mounting pressure. It is expected to provide answers to questions that condition the very possibility of effectively extending law enforcement into new territory. A prerequisite thereto is determining the applicable law and the competent authorities. Yet, technological developments generate seemingly de-spatialised settings in which activities appear to be located "everywhere and anywhere."[1] As a result, online content floats in the transnational open waters of the Internet, while crypto transactions sail the transnational waves of distributed ledgers.

Although this vision calls for several nuances, it is correct to the extent society is confronted with items hardly linked to a single jurisdiction. Consequently, they are also hardly subject to a clear set of legal provisions. To identify the applicable law, it is thus necessary to refer to conflict-of-law rules. However, these struggle to provide immediate and clear-cut answers when it comes to these technologically-bred creatures. The same applies to determining the competent jurisdiction.

Several elements are rendering the concerned rules ill-fitted when confronted with these technological evolutions. In the present contribution, the focus is on one specific element, namely pseudonymity.

This contribution specifically aims at explaining the state of art when it comes to transactions executed on distributed ledgers. The latter can be used for several purposes. Among these, the possibility of transferring crypto assets from one wallet to another attracts the most attention, particularly when it comes to transfers gone wrong, notably because of dysfunctional

1 As explained by Andrea Slane, "Tales, Techs and Territories: Private International Law, Globalization and the Legal Construction of Borderlessness on the Internet" (2008) 71 Law and Contemporary Problems 129, 129.

© ANNE-GRACE KLECZEWSKI, 2023 | DOI:10.1163/9789004514850_008
This is an open access chapter distributed under the terms of the CC BY-NC-ND 4.0 license.

smart contracts, or transfers made for the wrong purpose, such as money laundering.[2]

This contribution first explains pseudonymity as it can effectively be observed in the context of distributed ledgers (**2.**) and the different settings which may surround crypto transactions (**3.**). This allows the contribution to present the exact impact of such pseudonymity on PIL (**4.**), using European PIL as an example. Finally, this contribution emphasises an issue which can be even more fundamental than clarifying PIL, namely ensuring the possibility of effective enforcement of rendered judicial decisions (**5.**).

2 Pseudonymity

Distributed ledgers are generally presented as entailing pseudonymity. The latter is in turn presented as a source of potential hurdles and harms.

Notably, the Swiss Federal Assembly recently rejected a motion grounded on several misconceptions about pseudonymity in the crypto ecosystem and what it concretely entails.[3] The motion primarily proposed an obligation to identify the beneficial owner of cryptocurrencies based in Switzerland and the corollary prohibition of using cryptocurrencies that do not guarantee such identification. The asserted objective of the measure was to reduce the risk of criminal use of such cryptocurrencies. Beyond the vagueness of the notion of "cryptocurrency based in Switzerland," the motion could be further criticised as advocating in favour of a burden contrary to the nature of distributed ledger technology while overlooking the nuance between pseudonymity and anonymity. Identification points exist and are in many cases subject to anti-money laundering requirements, as recalled by the Federal Council,[4] and as further explained in this contribution.

2 A notorious example is the Dread Pirate Roberts, the pseudonym of the creator of the Silk Road and allegedly Ross Ulbricht from whom the FBI confiscated about 144,000 BTC, as these were received from illegal transactions such as drug dealing.

3 Motion 21.4068, "Cyber piraterie au détriment des entreprises et des collectivités publiques. Interrompre le circuit financier des rançons via les cryptomonnaies," submitted to the Swiss Federal Council by Roger Nordmann 22 September 2021, motion rejected by the Swiss Federal Council of 10 November 2021.

4 Opinion of the Swiss Federal Council dated 10 November 2021 regarding Motion 21.4068 <https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20214068> accessed 26 May 2022.

Pseudonymity was already a major issue at the beginning of the Internet. The development of Web 2.0, however, provided for partial solutions thereto.[5] It is still perceived as a major issue when it comes to distributed ledgers, but similarly, it may no longer be so, as more and more elements of the ecosystem nuance its practical effect.

2.1 *Public versus Private Distributed Ledgers*

The first element to be considered to assess the level of pseudonymity in a distributed ledger environment is the type of ledger at stake.

Distributed ledgers and blockchains are often used as synonyms. However, blockchains are rather a subcategory of distributed ledger technology ("DLT") which enable "parties with no particular trust in each other to exchange any type of digital data on a peer-to-peer basis with fewer or no third parties or intermediaries."[6] Blockchains are a subset of DLTs relying on cryptography to record data in "chains of blocks."[7] Accordingly, the initial presentation referring to technological developments may be misleading. Blockchains are not a technological novelty; rather, they are a novel combination of pre-existing technologies: the already mentioned distributed ledgers but also public-key encryption, Merkle tree hashing and consensus protocols.[8]

All distributed ledgers are not alike. Their constitutive elements may be modulated to suit different needs. Just like developers may prefer one coding language over another because of the possibilities related thereto,[9] developers may prefer one distributed ledger over another for precisely the same reasons. There is Ethereum but also Cardano, Polkadot, Hyperledger, Ripple and many more already existing or to come. No general definition of DLT reflects the wide-ranging diversity. Accordingly, Paolo Tasca and Claudio Tessone suggest a taxonomy which identifies the various components of blockchains and the relationships among them.[10]

---

5 Platforms emerged as centralisation points providing valuable identification information, and, at times, a blamable for negligent oversight, in lieu and place of the pseudonymous user whose activities they tolerated.

6 Amanda Anderberg et al., *Blockchain Now And Tomorrow*, Susana Figueiredo do Nascimento and Alexandre Roque Mendes Polvora (eds) (Luxembourg: Publications Office of the European Union, 2019), 13.

7 *Id.*

8 As reminded in Paolo Tasca and Claudio Tessone, "A Taxonomy of Blockchain Technologies: Principles of Identification and Classification" (2019) 4 Ledger 1, 2.

9 See the explanations in James Somers, "Toolkits for the Mind" (*MIT Technology Review*, 2 April 2015) <https://www.technologyreview.com/2015/04/02/168469/toolkits-for-the-mind/> accessed 26 May 2022.

10 Tasca and Tessone (n 8).

An important feature is the public or private character of the distributed ledger, as well as its permissioned or permissionless character. Based on the popular examples provided here above, public opinion generally has in mind an open ecosystem that anyone can join as a node and where anyone can insert new data, and similarly, anyone can retrieve data through publicly available scans such as Blockstream[11] or Etherscan.[12] These are referred to as "blockchains" *sensu strictu*. The broader category of distributed ledgers further encompasses private ecosystems to which participants must be accepted as nodes and where a network operator thus retains some power (private) and/or where the capacity to record data and/or read such data is limited to certain actors that have been pre-authorised (permissioned). Such ecosystems are built in-house or by external private actors offering them, for instance, on a software-as-a-service basis. A private distributed ledger could be conceived as permissionless, just like a public one could be permissioned.

This distinction is relevant to our point, as pseudonymity may be only partial on specific distributed ledgers. For instance, a private ledger operated by a corporation will often permit authorised people to access information allowing the unveiling of identities behind logs. Accordingly, the problem debated in the present contribution is not a general problem in the context of distributed ledgers. It mostly affects public blockchains, which are the most popular. As such, the following sections of this contribution will focus exclusively thereon.

2.2 *Pseudonymity versus Anonymity*

One of the advantages of blockchains, *i.e.*, public and permissionless distributed ledgers, is their transparency. All transactions are recorded and can be checked by anyone. For instance, by checking Etherscan or Polygon scan, anyone can discover the list of transactions recorded within a specific block, as well as the exact transfers of crypto assets performed by some of these transactions, from one particular public address to another. All involved addresses are visible, just like the type of transaction at stake.

However, in contrast to this high level of transparency for transactions, the precise identity of those executing the transactions is not readily available. Otherwise, few would use a service that is publicly displaying their every move. For example, on social media, one chooses which activity to post and with which level of privacy. On blockchains, it is the platform itself that "posts" information without asking, with a "visible to all" parameter by default.

---

11 See generally "Blockstream Explorer" (*Blockstream Explorer*) <https://blockstream.info> accessed 26 May 2022.

12 See generally "The Ethereum Blockchain Explorer" (*Etherscan*) <https://etherscan.io> accessed 26 May 2022.

FIGURE 6.1 Screenshot of a random public address on Ethereum, as displayed on Etherscan

Although the public address, usually in the form of a succession of numbers and letters, may appear to result in anonymity, it does instead provide mere pseudonymity.

To better grasp the nuance between both concepts, refer to the definition of pseudonymisation as contained in the General Data Protection Regulation:[13]

> the processing of personal data in such a manner that the personal data *can no longer be attributed to a specific data subject without the use of additional information*, provided that such additional information is *kept separately* and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.[14]

A public address operates precisely that way. If supported by additional elements, it could lead to the identity of its owner.

The public address, *i.e.*, a series of numbers and letters resulting from a hash, is nothing like usual identifiers, such as an identity card, which readily identifies a person, because a public address does not indicate whether there is even a real person behind it.

To generate a public address on Ethereum, the user needs to first use a secure hash algorithm in 256 bits, usually referred to as SHA256.[15] The private key chosen by the user is then transformed into a public key by applying yet another algorithm, Keccak-256. The public key is then turned into an Ethereum

13 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L 119/1 (hereafter "GDPR").

14 *Id.* at Article 4(5) (emphasis added).

15 See, *e.g.*, an online SHAH256 function can be found at "SHAH256" (*Online Tools*) <https://emn178.github.io/online-tools/sha256.html> accessed 26 May 2022.

address by adding 0x before the last 20 bytes of the result obtained through Keccak-256. The result is a line of 42 hex string characters.

One cannot perform an inverse computation unveiling the private key, and even if this was possible, one would still not know to whom it belongs. Yet, the public address never renders one completely anonymous, either, for at least two reasons.

On one hand, if coupled with other elements, it could lead to the identification of the person holding the private key, or at least the broader category to which it belongs. For instance, data scientists algorithmically cluster transactions to predict whether the public address belongs to an individual, an exchange, a miner, or is used for an ICO. Notwithstanding this example, with the clustering method alone, one is most often unable to couple the public address with the elements required to identify the precise holder of the associated private key. Because an individual can use several wallets, or, conversely, one wallet could be used by several individuals, pseudonymity is even greater, blurring traces for any attempt at clustering. Accordingly, if crypto assets are sent to an erroneous public address, often, there will be few methods of contacting the mistaken counterparty to arrange for a return.

On the other hand, the ecosystem of distributed ledgers is intertwined with numerous centralised intermediaries. As crypto assets are still seldom accepted as means of payment for daily transactions, one must convert crypto into fiat currency to effectively pay for a purchase. Here, know-your-customer and other anti-money laundering duties allow involved intermediaries to associate a public address with an identity.

2.3 *The Influence of Centralised Third Parties*

Beyond the case of conversion into fiat, the actual scope of pseudonymity in the context of distributed ledgers is further variable. The description made in the previous subsection is increasingly nuanced by the emergence of various centralised actors rendering the decentralised context more convenient. Such actors bundle the advantages of decentralisation with those of centralisation. Specifically, they partially oversee activities and may, under certain circumstances, intervene should problems arise.

Conversely, the description is also nuanced by specific projects aimed at shifting towards anonymity, such as Monero, ZCash, and some proposals by Ripple, to name just a few. However, for now, public distributed ledgers generally still provide pseudonymity rather than complete anonymity.

Here, the focus is on the first type of nuance and this section explains how some of the features added by centralised actors wither the scope of pseudonymity.

2.3.1 Wallets

In theory, each user has its own public address serving as a wallet, where assets are deposited and readily available for transactions.[16] In addition to the wallet address, what is commonly referred to as a wallet is the application (comparable to a banking application) allowing one to access and manage the content of one or even several wallet addresses, such as *Metamask* on Ethereum.

In practice, centralised actors do often rely on omnibus wallets, to which users transfer their assets which are pooled together therein. Thus, there is one wallet controlled by the intermediary where assets are held for the account of users. The individualisation of such jointly held assets is achieved through parallel mechanisms, such as, for instance, private blockchains or a traditional database. Considering that platforms usually identify their users, the involved parties will normally be known should a mistake or claim arise out of a transaction executed through an omnibus wallet.

Again, in theory, each user is the only one able to initiate a transaction with his/her private key associated with the non-custodial wallet address. By now, most centralised actors rely on custodial wallets, whether these are individualised on-chain or merely portions of an omnibus wallet.

Private keys allowing transactions on assets held in such custodial wallets are held by the centralised intermediary. Therefore, while users have the power to directly initiate transactions on assets held in non-custodial wallets, they lose the power to do so once their assets are deposited in custodial wallets. Under a custodial setting, subsequent transactions with assets held in these wallets occur based on orders submitted to the platform, which executes them, whether on an execution-only or discretionary basis. As a result, based on its terms of service, the platform could refuse to execute an order deemed erroneous or suspicious. Of course, this system also has its flaws.

A relevant example of this is the prominent case of the Bitfinex hack which occurred in 2016. Although the exact reasons which allowed it to happen have not been clarified over the years, commentators have, notably, emphasised the multi-signature wallet used by Bitfinex. As related by the press, "some observers have blamed the service for 'blindly signing' the withdrawal of nearly

16 There are at least two types of public addresses on distributed ledgers. The most known addresses are used as a wallet for tokens (wallet addresses are also referred to as externally owned addresses or "EOA") but some addresses host smart contracts (contract address). The latter addresses are created each time a programmer effectively deploys the code of a smart contract onto the blockchain.

120,000 BTC and wondered why no potential countermeasures were in place in the event of a movement of funds of that size."[17]

Therefore, considering the foregoing, if the platform resorts to an omnibus account or obtains the power of disposal over individual accounts held by users, a centralisation point exists.

2.3.2 Financial Intermediaries

Centralised intermediaries are involved in many more ways than merely making wallets available for the storage of crypto assets, or as previously mentioned, acting as converters into fiat. They may also offer various financial services.

Popular centralised intermediaries act as exchanges or investment platforms, for example, Binance, Kraken, Bitstamp or SwissBorg. Others provide more complex services.

Usually, an identification procedure is required by such intermediaries before the user can access the service, because these intermediaries mostly fall within the scope of anti-money laundering regulations (see *infra* point 2.4). Their intervention renders the existing chain scanners more useful. Transactions involving public addresses identified by centralised intermediaries are recorded on-chain like any other transactions. Upon request, the intermediary may unveil the identity of the owner of such public address, for example, an address which was blacklisted because of its involvement in a scam.[18]

Such requests must comply with applicable laws, and it may require a lengthy process in international cases. In Switzerland, intermediaries are not entitled to communicate data to foreign public authorities unless they received an official request from a competent foreign authority (for instance, a court). Article 271 al.1 of the Swiss Criminal Code makes it a criminal offence to communicate user information on the mere grounds of an informal letter.

2.3.3 Conversion into Fiat Currencies

As already mentioned, another point at which identification usually occurs is when the user wishes to spend his or her crypto assets for a traditional purchase

17 Stan Higgins, "The Bitfinex Bitcoin Hack: What We Know (And Don't Know)" (*CoinDesk*, last updated 14 September 2021) <https://www.coindesk.com/markets/2016/08/03/the-bitfinex-bitcoin-hack-what-we-know-and-dont-know/> accessed 26 May 2022.

18 See *e.g.*, in the United Kingdom, *AA v Persons Unknown & Ors, Re Bitcoin* [2019] EWHC 3556 (Comm) (13 December 2019). During this case, following an analysis of the chain to identify wallets involved with the proceeds of a hack, a request was made to identify the owner of a wallet linked to Bitfinex.

of goods and services. For now, one is still forced to convert into fiat currencies and withdraw these from the wallet to a traditional bank account or onto a credit card, as only a few places accept payments made directly in crypto.[19]

Consequently, anyone who currently has a fortune in crypto but desires to remain pseudonymous is restricted in his or her use of such fortune for spending purposes. Things may change over time, as some projects aim at tokenising real estate, while others aim at rendering crypto payments possible for routine spending through service providers similar to PayPal (the latter itself having integrated crypto).

2.4 *Anti-Money Laundering Requirements*

Centralised intermediaries will generally be subject to local anti-money laundering regulations, whether on the occasion of performing transfers, accepting deposits, or other regulated activities.

A concrete example of such regulations applicable to crypto actors can be found in the AML framework applicable in a jurisdiction depicted as fostering the crypto scene, probably less restrictive than some other jurisdictions, and therefore attracting many crypto actors: Switzerland.

Under the Swiss Anti-Money Laundering Act ("AMLA")[20] and Ordinance ("AMLO"),[21] holding crypto assets on deposit on a professional basis, in whatever form it is, and regardless of whether such deposit is deemed a regulated activity by the Banking Act, renders one a financial intermediary subject to anti-money laundering obligations.[22]

---

19 *E.g.*, in Switzerland, see "galaxus.ch" (*Galaxus*) <http://galaxus.ch/> accessed 26 May 2022; internationally, this was temporarily the case with Tesla and recently became the case with Gucci.

20 Federal Act on Combating Money Laundering and Terrorist Financing of 10 October 1997 (Anti-Monkey Laundering Act, AMLA), RS 955.0 (hereafter "AMLA").

21 Federal Ordinance on Combating Money Laundering and Terrorist Financing of 11 November 2015 (Ordinance on Anti-Money Laundering), RS 955.01 (hereafter "AMLO").

22 Pursuant to Article 2(3) of the AMLA, the anti-money laundering requirements apply to anyone who "on a professional basis accept or hold on deposit assets belonging to others or who assist in the investment or transfer of such assets." The latter are deemed to be financial intermediaries for the purpose of the law. The article specifically lists, in a non-exhaustive manner, examples of encompassed activities. Since the categories clarified by the AMLO are merely exemplative, holding crypto assets on behalf of clients in principle falls within the broader scope of "holding on deposit assets belonging to others," regardless of whether such activity matches one of the examples. The Swiss Financial Market Supervisory Authority (hereafter "FINMA") expressly confirmed this interpretation by indicating that being a custody wallet provider renders one subject to the AMLA (*cf.* FINMA, "Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)," (*FINMA*, 16 February 2018) <https://www.finma.ch/~/media/finma

Moreover, issuing crypto assets categorised as payment tokens is deemed an issuance of means of payment and similarly renders one a financial intermediary.[23]

Issuing security tokens would also result in being a financial intermediary, whether because they are issued by a securities house[24] or because such securities are held and managed by the issuer.[25]

Compliance with AML requirements is also highly recommended when issuing utility tokens, at least if payments should be made in fiat. Indeed, the Practical Guide of the Swiss Bankers Association on the opening of corporate accounts for companies active in the DLT sector recommends that:

> if the existing corporate account is also used for financing and issuing tokens financing and token issuance, it is the bank's responsibility to take operational measures to ensure that funds from the issuance of tokens can be made freely available to the customer only after a thorough check. The bank does not carry out any legal analysis of the nature and maturity of the tokens and considers a priori that the issuer is subject to the AMLA. If this is not the case, it is up to the issuer to make this known and justify

/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?sc_lang=en&hash=C9899ACF22747D56C800C6C41A7E28AB> accessed 26 May 2022 (hereafter "FINMA Guidelines").

23 Services related to payment transactions as encompassed by the scope of the AMLA are substantiated at Article 4 of the AMLO. Pursuant to the AMLO at paragraph (1), "[a] service in the field of payment transactions within the meaning of Art. 2 Para. 3 letter b AMLA exists in particular if the financial intermediary (…) c. issues or manages non-liquid means of payment which the contracting partner uses to pay third parties." According to 1bis(c) of the AMLO, non-liquid means of payment include "virtual currencies which are actually used or intended by the organizer or issuer to be used as a means of payment for the acquisition of goods or services or which are used for the transmission of money or value." Note that if the payment system is of systemic importance, it will fall within the scope of Article 4(2) of the Federal Act on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading of 19 June 2015 (Financial Market Infrastructures Act), be subject to a specific license, and ultimately be deemed as a financial intermediary based on Article 2(2) of the AMLA, rather than the more catch-all Article 2(3). This in turn has a concrete impact on the scope of requirements to which the intermediary is subject. For regulated intermediaries listed under Article 2(3), details are specified in the Ordinance of the Federal Market Supervisory Authority on Combatting Money Laundering and Terrorist Financing in the Financial Sector (FINMA Anti-Money Laundering Ordinance), RS 955.033.0. For the remaining intermediaries, these details are relatively freely determined by themselves along with a self-regulatory organisation to which they need to affiliate.

24 Subject to the AMLA pursuant to Article 2(2)(dter).

25 Subject to the AMLA pursuant to article 2(3)(g).

> it. In case of doubt, one means of proof may be FINMA's response to a question on the matter.[26]

As a result, lacking AML compliance, it would be highly difficult to open a bank account to collect proceeds from the sale.

Finally, executing conversions[27] or on-chain transfer orders placed by a client[28] also turns one into a financial intermediary in the meaning of AMLA.

Similar rules, or even more extensive ones, apply in other jurisdictions. As a result, most centralised intermediaries in the crypto field, regardless of their location,[29] will in one way or another end up subject to anti-money laundering requirements and therefore perform a KYC, KYB or even KYT. Therefore, crypto transactions executed by their clients will no longer benefit from the veil of pseudonymity usually associated with wallet addresses.

2.5 *Intermediary Conclusion*

If distributed ledger transactions were initially designed under the veil of solid pseudonymity, subsequent evolutions in the blockchain ecosystem brought back centralisation. As a result, pseudonymity remains at the surface, but it is only conditional.

The few scenarios where pseudonymity still hinders any attempts at judicial claims are similar to those existing off-chain:

If one sends money to the wrong address, it is like losing a banknote on the street. If one contracts with a dubious party and pays in crypto assets, it is like purchasing from a scam online store.

---

26 Swiss Bankers Association, "SBA guidelines on opening corporate accounts for DLT companies" (*SwissBanking*, August 2019) <https://www.swissbanking.ch/_Resources/Persistent/8/2/0/e/820ecd3799e43523b91c7c3f65122e97f9a85601/SBA_guidelines_on_opening_corporate_acounts_for_DLT_companies_2019_EN.pdf> accessed 26 May 2022.

27 Pursuant to Article 2(3)(c) of the AMLA.

28 Pursuant to Article 4(2) of the AMLO "The transmission of money or value means by accepting cash, precious metals, virtual currencies, virtual currencies, cheques, or other payment instruments and then (a) paying the equivalent sum in cash, precious metals or virtual currencies, or (b) without cash, executing a transmission or transfer through a payment or clearing system."

29 An exception is if the centralised intermediary is located in jurisdictions that are deemed to have a malfunctioning anti-money laundering system or defective application thereof, as is the case of those included on the blacklist of the Financial Action Task Force (which in March 2022 still lists merely two countries: Iran and the Democratic People's Republic of Korea). See Financial Action Task Force, "High-risk and other monitored jurisdictions" (*FATF*) <https://www.fatf-gafi.org/countries/#high-risk> accessed 26 May 2022.

The major difference between the off-chain scenarios and their on-chain equivalents is the difficulty of circumventing the absence of an identified defendant. Transactions executed on-chain cannot be reversed by anyone and there are few, if any, equivalents to the reimbursement procedure by a marketplace hosting the scam account or a credit card company cancelling an authorisation.

3 Transacting on Distributed Ledgers

Transactions can rely on distributed ledgers in several ways. They can be fully contained in the DLT environment (**3.1.**), but they can also merely operationalise off-chain relations between parties knowing each other (**3.2.**). Problems related to such transactions can be of various types and, likewise, crystalise on-chain but also off-chain (**3.3.**). It is yet relevant to focus on a specific type of problems, namely DeFi scams (**3.4**). The latter are highly mediatised but, as subsequently explained, they do not necessarily challenge PIL the most.

3.1 *On-chain Only*

Distributed ledgers allow transactions which are fully contained therein. A textbook example would be the following: the holder of public address A transfers crypto assets to address B. Holders of both addresses do not know each other off-chain, or offline, and thus cannot effectively communicate should a dispute regarding the transfer arise.

A practical example of this is the case of Laszlo Hanyecz, the first individual to use bitcoin (BTC) for a commercial transaction.[30] Laszlo published on an online forum an offer to pay 10'000 BTC to whomever accepted to bring him two large pizzas. Once the BTC was sent to the public address communicated by the forum member who signed up for the task, should the forum member not deliver the pizzas, it would have been impossible for Laszlo to seek reimbursement. Further, any forum member could disappear by deleting his/her account, which was also protected by a nickname dissimulating whoever he/she was.

Such situations are cumbersome challenges for PIL but are not typical of the distributed ledger environment; distributed ledgers merely add to the issue. If

30 See Galen Moore, "10 Years After Laszlo Hanyecz Bought Pizza With 10K Bitcoin, He Has No Regrets" (*CoinDesk*, 22 May 2020) <https://www.coindesk.com/markets/2020/05/22/10-years-after-laszlo-hanyecz-bought-pizza-with-10k-bitcoin-he-has-no-regrets/> accessed 26 May 2022.

contractual claims arising out of pseudonymous interactions online are not new, payment means available until now rendered the veil of pseudonymity thinner. Bank accounts, credit cards, PayPal, and other usual means require identification. Maintaining pseudonymity would require tricking these means by using fake identities. The latter is much more complicated than sending crypto funds through distributed ledgers where pseudonymity still operates to a variable extent, as previously explained. Therefore, for example, the dark net quickly adopted distributed ledger transactions as those suited the needs of its users.

3.2 *Off- and On-chain*

Many crypto transactions recorded on-chain are merely the execution of a traditional contract, whether taking the form of terms of service applicable to a specific service, or of a custom contract between determined parties, such as, for instance, a token purchase agreement.

This is notably the case of: orders placed on crypto exchanges (*e.g.*, X decides to convert ETH in MATIC); private and public token sales (*e.g.*, X decides to purchase a brand-new utility token directly from its issuer); and/or crypto payments for off-chain goods and services (*e.g.*, X decides to accept a payment in USDC when selling his car second hand).

3.3 *Possible Problems*

Issues can arise in various forms. The on-chain execution of a transaction can be corrupted because of a human or system error. The transaction could also be the victim of a hack.[31] Execution could also be contested based on off-chain issues regarding the terms of the contract underlying the on-chain execution or the erroneous translation into code of an agreed clause. Moreover, issues can arise from a tripartite relation whose terms were unclear, especially regarding the exact role and liability of the intermediary.

3.4 *A Concrete Example: DeFi Scams*

Smart contracts can be defined as software code immutably stored on a distributed ledger and allowing for the automatic execution of predefined functions. Whether smart contracts are contracts from a legal standpoint is an ongoing debate. Regardless of the considerations raised against such characterisation,

31 Wolfie Zhao, "Poly Network attacker returns $256 million of the stolen cryptocurrency" (*The Block*, 11 August 2021) <https://www.theblockcrypto.com/post/114189/poly-hack-attacker-return-funds-id-slowmist> accessed 26 May 2022.

smart contracts are increasingly popular because they offer a technical solution to a major legal problem, namely non-performance of contractual obligations.

The appeal of resorting to smart contracts, whether as stand-alone contracts or technical translations of off-chain contracts, stems from at least two elements. One, it is convenient to rely on an algorithm automatically executing obligations as soon as specified conditions are irrefutably met. It results in payments being processed without further debate or certificates being transferred without further delay. Two, it is reassuring to know that such an algorithm is safely stored at a contract address on a distributed ledger guaranteeing immutability.[32] The said immutability counters most *ex-post* objections, such as refutation or distortion of previously agreed terms.

Decentralised Finance relies precisely on such. Decentralised Finance Protocols, generally referred to as DeFi, are aggregates of intertwined smart contracts. They constitute the best example of triangulation, where triangulation maintains the pseudonymity issue.

The term DeFi encompasses a broad array of services, ranging from decentralised exchanges (ex. Uniswap) to decentralised (crowd)lending (ex. Aave). In each case, the centralised intermediary has been removed and replaced by smart contracts, which are automatically executing tasks. The intermediary thus becomes technological and in principle, autonomous or at least decentralised.

This inference is nuanced. Smart contracts are stored on the ledger, and they are, like any other data, such as crypto assets, stored at a public address. Each contract address, as any public address, has a private key. Anyone who deploys a smart contract ends up with the private key of the address generated on this occasion. He or she could subsequently transfer it, destroy it, or restrain its use, whether contractually (by, for instance, subjecting decisions regarding the smart contract to decentralised governance) and/or technically (by placing the private key in storage with limited access rights, resulting in the DeFi protocol being mostly autonomous).

As a result, there is, in practice, although indirectly, a centralisation point which could be deemed responsible for the operations of the smart contract. This point could be a single person or a group should the key be split[33] or

32 The smart contracts stored on the distributed ledger should be distinguished from the protocol running the distributed ledger, which could also be referred to as an algorithm.

33 One key can be split in multiple pieces which need to be assembled in order to produce a signature.

should it be a multi-signature wallet.[34] These are often the project developers whose names are seldom made public.

Alternatively, the key could be destroyed to ensure the protocol is truly autonomous. Such a solution renders it impossible to tamper with the smart contract, but it also prevents anyone from intervening for legitimate reasons (such as, for instance, fixing a glitch). It must be clarified that despite the immutability of smart contracts deployed on the distributed ledgers, alternative paths exist to perform updates and corrections, all of which will themselves be recorded as transactions visible on the ledger. Moreover, some crucial functions of the smart contract could be reserved exclusively for those holding the admin keys.

Considering the foregoing, rather than guaranteed decentralisation, as suggested by its name, DeFi merely provides automation. Concrete decentralisation of DeFi will be ensured mostly by involving token holders in votes relating to the maintenance and development of the protocol or even delegating these decisions to them. Nevertheless, there are usually no foreseeable means to ensure only decisions validly adopted by token holders can be implemented. Private keyholders could go against all parties and implement unapproved changes.

Conversely, centralised finance protocols, so-called CeFi, expressly acknowledge the existence of key holders having ultimate control over smart contracts. The private keys are held by the corporation endorsing its role as a technology (and sometimes financial) service provider, although the services are, effectively, provided by smart contracts. This is the case with the most popular exchanges, among which are Coinbase and Binance.

The presence of a *de facto* centralised control point in DeFi is evidenced at the occasion of scams, to which the DeFi environment is increasingly subject.

One type of scam is a smart contract scam: developers include the foundations of the scam in the code itself, by means of an inflation bug, transfer of ownership, or access revoking. Although the code is publicly available, not every user bothers to check each line, nor is he/she necessarily able to understand it. This allows several exit scams to occur. For example, one of them was the alleged Meerkat Finance scam: the operators claimed its smart contract was compromised and drained $31 million worth of crypto assets the day following its launch.[35]

---

34 A wallet requiring several private keys to sign a transaction.

35 Jamie Crawley, "DeFi Project Meerkat Raises Eyebrows With Claimed $31M Hack a Day After Launch" (*CoinDesk*, 4 March 2021) <https://www.coindesk.com/policy/2021/03/04/defi-project-meerkat-raises-eyebrows-with-claimed-31m-hack-a-day-after-launch/> accessed 26 May 2022.

Another type of scam is referred to as a rug pull. These are set up by creating a token listed on a decentralised exchange such as Uniswap, Sushiswap, or Pancakeswap, where, due to their decentralised nature, there is no one in charge of verifying the token prior to its listing. Once the listing is running and pairs exist with established crypto assets (for instance, token/BTC or token/USDC), users buy the crypto asset up to the point where the creators of the crypto asset decide to empty the exchange pool. This drives its price to zero.

To understand rug pulls, it is necessary to understand liquidity pools. Each pool is a trading venue for a pair of tokens. When a pool contract is created on an exchange, the balance of each token is zero. To begin facilitating trades, someone must seed the pool with an initial deposit of each token. This deposit sets the initial price for trading. When trades begin, the pool grows.

The creators of the TRUAMPL token (ticker TMPL) operated such a rug pull. They added liquidity to create a TMPL/ETH market. Once actual users entered the market, the creators withdrew the initially added percentage of liquidity, and by doing so, drained liquidity out of the market.

Finally, as a reminder, the shield of pseudonymity operates both ways. In specific cases, it could be the users, not the developers, who are to blame. In October 2021, a protocol error upon upgrade led to a distribution of $90 million dollars in value to users of Compound, an autonomous interest rate protocol.[36] Although such distribution results in what many legal systems refer to as unjust enrichment, since the protocol knew only the public addresses of its users, not their identity, there was no way to force them to return the funds. The founder had to rely on users' good faith to recover millions of dollars.

4 The Impact on PIL

The crux here is how pseudonymity hinders the effectivity of PIL when its principles rely on the country of habitual residence of a party. Usually, if the principles point at the country of the claimant, there will be no issue to the extent one must identify him or herself to bring the claim to court. Problems arise where the principles point to the country of the defendant or at the location of the transaction itself. The focus here is exclusively on the first.

Imagine a situation where programmers who orchestrated a scam are known. PIL can then provide the expected answers. However, as previously

36 MacKenzie Sigalos, "DeFi bug accidentally gives $90 million to users, founder begs them to return it" (*CNBC*, 1 October 2021) <https://www.cnbc.com/2021/10/01/defi-protocol-compound-mistakenly-gives-away-millions-to-users.html> accessed 26 May 2022.

mentioned, often the identity of those who set up the protocol remains unknown. If users sent funds to the protocol directly from their non-custodial individual wallet address, not much can be done for as long as the defendant remains a mystery. If users sent funds through a CeFi provider, things may be different. Indeed, many centralised exchanges offer access to selected DeFi protocols. There, they mostly operate as technical gateways. Their terms of service traditionally exclude, to the extent permitted by law, any liability for such external DeFi protocols to which clients are redirected at their own risk. Terms of service specify the law and the jurisdiction applicable to claims arising out of their content. Accordingly, in the event of intentional or gross misconduct, such as recommending DeFi protocols that are obvious scams, the contractual limitation of liability could be set aside by the applicable law, and issues stemming from the pseudonymity of protocol developers would similarly be set aside. In most cases, however, the limitation of liability holds.

In the present section, the issue resulting from the pseudonymity of a defendant is specifically illustrated by outlining provisions of European PIL regarding the applicable law.

4.1 *Tort*

In the event of an international extra-contractual situation, whether based on criminal activity or not, solutions are, in principle, to be found in Regulation (EC) No 864/2007 of the European Parliament, and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (hereafter "Rome II").

As a preliminary remark, note that Rome II excludes from its scope "non-contractual obligations arising under bills of exchange, cheques and promissory notes and other negotiable instruments to the extent that the obligations under such other negotiable instruments arise out of their negotiable character."[37] Therefore, it is important to always assess the object of the problematic transaction. If it is a transfer of crypto assets, the nature of such crypto assets must be analysed to determine whether they could be deemed security tokens[38] rather than mere utility or payment tokens. More specifically, it must

37 Regulation (EC) No 864/2007 of the European Parliament, and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II), [2007] OJ L 199/40, Article 1(2)(c) (hereafter "Rome II").

38 For instance, the FINMA Guidelines (n 22) and FINMA's "Supplement to the guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs)" (*FINMA*, 11 September 2019) <https://www.finma.ch/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-stable-coins.pdf?sc_lang=en&hash=178A9017323F2FB01B195BA446F41F19> (hereafter "FINMA Supplement") in

be assessed whether it is a negotiable instrument in the meaning of relevant financial laws. In the affirmative, different principles are to be applied to determine the applicable law. In the negative, one can proceed with the principles contained in Rome II.

Rome II relies on the country where the direct damage occurred, *i.e.*, the *lex loci damni*,[39] to be understood as the country where the personal damage was sustained. The place where the damage effectively crystallised could, in many cases, point at the residence of the claimant[40] or the country where the property was damaged. As a result, Rome II appears to accommodate situations related to crypto transactions without any additional hurdles.

By means of comparison, things are quite different under the Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters ("Brussels I"). Therein, the general rule is that "persons domiciled in a Member State shall, whatever their nationality, be sued in the courts of that Member State."[41] Specifically for tort, delict, or quasi-delict, it is foreseen that the defendant may be sued "in the courts for the place where the harmful event occurred."[42] In theory, the criterion becomes the same under Brussels I as under Rome II when determining the applicable law. In practice, however, this is not the case.

Indeed, the European Court of Justice specified that when the place where the event giving rise to the damage and the place where the damage effectively crystallised are not identical, the expression "place where the harmful event occurred" within the meaning of Article 5(3) of the Brussels Convention may

---

Switzerland provide indications regarding how to categorise a token. According to FINMA, "asset tokens represent assets such as a debt or equity claim on the issuer. Asset tokens promise, for example, a share in future company earnings or future capital flows. In terms of their economic function, therefore, these tokens are analogous to equities, bonds, or derivatives. Tokens which enable physical assets to be traded on the blockchain also fall into this category."

39 Rome II (n 38), Article 4(1); see also Rome II (n 38), Recitals 16 and 18.

40 See the Commission of the European Communities, "Proposal for a Regulation of the European Parliament and the Council on the Law Applicable to Non-Contractual Obligations ('Rome II'): Explanatory Memorandum" [2003] OCD 2003/0168, 14 (hereafter "Explanatory Memorandum").

41 Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, [2012] OJ L 351/1, Article 4(1) (hereafter "Brussels I").

42 *Id.*, Article 5(3).

cover both places.[43] As a result, the claimant has an option. Nonetheless, in a later case, the Court emphasised that:

> the expression 'place where the harmful event occurred' does not refer to the place where the claimant is domiciled or where 'his assets are concentrated' by reason only of the fact that he has suffered financial damage there resulting from the loss of part of his assets which arose and was incurred in another Contracting State.[44]

Although one of the two connecting factors may well point at the jurisdiction of the claimant,[45] it will not point at this jurisdiction based on the mere fact that some of the negative consequences of damage which initially crystallised elsewhere are felt in that jurisdiction.

The position of the Court is generally understood as the Court being against any interpretation of Brussels I that would make it more likely that a claimant sues in the courts of its own domicile. This position is in line with the general principle of Brussels I. However, it is not necessarily required under Rome II.

When confronted with a transaction localised on-chain, the event giving rise to the damage is hardly related to a single determined jurisdiction (unless it is a private blockchain, in which case the nodes and operators could, in some cases, be geographically concentrated) and/or the place where the damage effectively crystallised, if deemed on-chain, potentially points to the law of no specific jurisdiction. Therefore, it is a welcome outcome to fall back on the jurisdiction in which the claimant is located and/or where he was located when using the private key to sign the transaction which resulted in the damage.

However, the above solution results in damages from one scam being potentially subject to an extensive list of different legislations, rendering any collective action difficult.[46]

---

43 *Handelskwekerij G. J. Bier BV v Mines de potasse d'Alsace SA*, Judgment of the Court of 30 November 1976, Case 21–76.

44 *Rudolf Kronhofer v Marianne Maier and Others*, Judgment of the Court (Second Chamber) of 10 June 2004, Case C-168/02.

45 *Id*., para. 35.

46 This downside is expressly emphasised in the Explanatory Memorandum, which states: "The rule entails, where damage is sustained in several countries, that the laws of all the countries concerned will have to be applied on a distributive basis, applying what is known as 'Mosaikbetrachtung' in German law." Explanatory Memorandum (n 41), 11.

Besides, this general principle has several exceptions in the form of specific rules applicable to situations where the latter principle does not allow a reasonable balance to be struck between the interests at stake.[47]

For instance, this is the case of unjust enrichment which is (i) subject to the law of the concerned relationship, whether a contract or tort, or alternatively, should it be impossible to determine such law and the parties do not have their habitual residence in the same country, (ii) subject to the law of the country in which the unjust enrichment took place.[48] Finally, it could also be the law of the country with which the situation is manifestly more closely connected.[49] The latter option could also be a welcome solution in many cases.

4.2 *Contractual Relations*

Many of the usual problems will arise in the context of transactions relying on an agreement, such as for instance, the sale and ensuing consensual transfer of crypto assets to a public address of the buyer. Such problems could usually be related to the amount sent (like the wrong amount provided, the wrong exchange rate applied, *etc.*) or the absence of the agreed counterpart (like the service or good not being provided despite payment being done).

Therefore, it is relevant to analyse the concrete magnitude of the pseudonymity problem based on Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (hereafter "Rome I"). Contrary to Rome II, solutions provided therein are partially thwarted when facing pseudonymity.

4.2.1 Choice of Law

Article 3 Rome I establishes freedom of choice as the basic principle.[50] Such choice shall, however, "be made expressly or clearly demonstrated by the terms of the contract or the circumstances of the case."[51] This requirement is not to be underestimated as, for instance, it implies that "the choice of the forum [...] does not per se imply a tacit choice of law but should be regarded as one of the

47 Rome II (n 38), Recital 19.

48 *Id.*, Article 10(3).

49 *Id.*, Article 10(4).

50 Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), [2008] OJ L 177/6, Article 3(1) (hereafter "Rome I").

51 *Id.*

factors to be taken into account when determining whether a choice of law is demonstrated with reasonable certainty."[52]

Moreover, when it comes to business-to-consumer contracts, parties may choose the law applicable to a contract but "such a choice may not, however, have the result of depriving the consumer of the protection afforded to him by provisions that cannot be derogated from by agreement by virtue of the law which, in the absence of choice, would have been applicable"[53]

Note that the above protection does not apply to:

> rights and obligations which constitute a financial instrument and rights and obligations constituting the terms and conditions governing the issuance or offer to the public and public take-over bids of transferable securities, and the subscription and redemption of units in collective investment undertakings in so far as these activities do not constitute the provision of financial service.[54]

Accordingly, anyone involved in transactions entailing crypto assets deemed to be securities should pay attention, particularly to any choice of law provisions included in the terms and conditions to which they agree.

Should the on-chain transaction, whether manual or automated by a smart contract, be the mere execution of an off-chain agreement, the parties may have specified the applicable law therein.

This seems the best scenario to the extent it *a priori* sets aside the issue of determining the applicable law. Nevertheless, this scenario is not necessarily picture perfect, as the initially made choice could be *a posteriori* contested.

The consent given to a choice of law should meet the existence and validity requirements stemming from Articles 10, 11 and 13 Rome I.[55] Should the choice of law be performed on-chain, pseudonymity may cause a problem considering the above-listed articles and render any choice of law invalid.

To illustrate the above, imagine a scenario in which a public address A sends a non-fungible token to address B, and the metadata of said token contains the hash or a link to standard terms or to a specific agreement with a choice of law clause included therein, but without any specification of the parties beyond a reference to the involved public addresses.

---

52 *Id.*, Recital 12; Paolo Bertoli, "Choice of Law by the Parties in the Rome II Regulation" (2009) 3 Rivista di Diritto Internazionale 697.

53 Rome I (n 51), Article 6(2).

54 *Id.*, Article 6(4)(d).

55 *Id.*, Article 3(5).

Article 11 Rome I determines the applicable law to verify the formal validity of a contractual choice of law. The solution differs depending on whether both parties to the contract are located in the same country. Thus, the first issue stemming from pseudonymity is establishing which standard applies, and it is not an easy task to identify the location of parties hiding behind a public address.

If they are in the same country at the time of the conclusion of the contract, the choice "is formally valid if it satisfies the formal requirements of the *law which governs it in substance under this Regulation* or of the law of the country *where it is concluded*."[56] Alternatively, if they are located in different countries at the time of the conclusion of the contract, it is "is formally valid if it satisfies the formal requirements of *the law which governs it in substance under this Regulation*, or of the law of either of the *countries where either of the parties or their agent is present* at the time of conclusion, or of the law of the country where either of the parties had his habitual residence at that time."[57]

Based on the above, if the defendant cannot be identified, the applicable law will be the one substantially governing the contract under Rome I. It must be questioned what to do if said law requires identifying the defendant.

In the case of business-to-consumer contracts, the formal validity is governed "by the law of the country where the consumer has his habitual residence."[58] This would be extremely convenient, as it would result in the law of the claimant easily being rendered applicable. The absence of an identified party, however, results in a *de facto* impossibility of assessing whether the defendant acted in the course of his/her personal or professional matters. Thus, this rule may, in practice, be seldom used when the pseudonymity of a party is involved unless the professional capacity of a defendant, notably with respect to large-scale DeFi scams, is inferred from the circumstances.

4.2.2 Absence of Choice of Law

In the absence of choice, Article 4(1) foresees the following connecting factor: "a contract for the sale of goods shall be governed by the law of the country *where the seller has his habitual residence*"[59] and "a contract for the provision of services shall be governed by the law of the country *where the service provider has his habitual residence*."[60]

56 *Id.*, Article 11(1).
57 *Id.*, Article 11(2) (emphasis added).
58 *Id.*, Article 11.
59 *Id.*, Article 4(1)(a).
60 *Id.*, Article 4(1)(b).

For example, utility tokens can be considered as services to the extent they are comparable to vouchers, chips, or keys that can be redeemed for contractually owed on-chain services.[61] When they are sold directly by their issuer, Article 4(1) can be relied upon. This being said, in principle, the issuer does conduct a token sale based on contractual documents with a choice-of-law clause. When it comes to subsequent transfers of utility tokens between users, it must be determined whether the contract can be deemed similarly governed by the above principle.

In the affirmative, it would be a convenient manner to circumvent any issues stemming from the pseudonymity of the defendant.

In the negative, it would be necessary to fall back to the default principle, "the contract shall be governed by the law of the country where *the party required to effect the characteristic performance of the contract has his habitual residence*,"[62] unless "it is clear from all the circumstances of the case that the contract is manifestly more closely connected with a country"[63] other than that one. Such a connecting factor is impossible to apply should the concerned party be pseudonymous. Therefore, it would be necessary to ultimately rely upon the law of the country with which the contract is most closely connected.[64] In turn, this may be a way to circumvent the issue, but at the cost of a lengthy and complex assessment to be performed by the Court.

Furthermore, Rome I foresees that:

> a contract concluded within a multilateral system which brings together or facilitates the bringing together of multiple third-party buying and selling interests in financial instruments, as defined by Article 4(1), point (17) of Directive 2004/39/EC, in accordance with non-discretionary rules and governed by a single law, shall be governed by that law.[65]

However, for now, most tokens are not security tokens and therefore are not traded by such systems.

Finally, in the case of business-to-consumer contracts where no choice of law is selected, these are in principle:

61 FINMA Guidelines (n 22), 3.
62 Rome I (n 51), Article 4(2) (emphasis added).
63 *Id.*, Article 4(3).
64 *Id.*, Article 4(4).
65 *Id.*, Article 4(4)(h).

> governed by the law of the country *where the consumer has his habitual residence*, *provided that the professional*:
>
> (a) pursues his commercial or professional activities in the country where the consumer has his habitual residence, or
> (b) by any means, directs such activities to that country or to several countries including that country, and the contract falls within the scope of such activities.[66]

As previously mentioned, although this is a convenient principle, it may be difficult to determine whether the above criteria are met in a specific case.

4.2.3 Intermediary Conclusion

Considering the above, it appears that the impact of pseudonymity varies depending on whether there is a choice of law clause.

In principle, pseudonymous parties, identified exclusively by their public address, could foresee a choice-of-law clause inserted in the metadata of the sold crypto asset (especially when it comes to non-fungible tokens), or of a smart contract executing the transaction. In such cases, identifying the jurisdiction of the parties would be relevant only to the extent the choice of law is contested, and identifying the jurisdiction of the defendant specifically may not be necessary considering the criteria to be applied.

In the absence of a choice of law, a setting which, for now is, unfortunately, the most common, especially in decentralised settings (or at least those presenting themselves as such), the pseudonymity of the defendant is much more problematic. It is even more problematic if the defendant can hardly be deemed as a professional, and as a result, the principles favourable to claimants as foreseen for business-to-consumer relations are not applicable. In this respect, existing principles are a major bottleneck for PIL and the possibility of effectively enforcing any legal provisions, whatever these may be.

5 A Problem Greater than PIL

If the applicable law is identified based on PIL despite pseudonymity, and the competent jurisdiction applies it (other problems may arise at this stage),

66 *Id.*, Article 6(1)(a)-(b) (emphasis added).

the judgement may still ultimately turn out difficult or impossible to enforce because the defendant remains pseudonymous at that point.

Blockchains are decentralised, and transactions recorded thereon are immutable. Accordingly, "correcting" a wrongly executed transaction requires the intervention of the defendant to generate a reverse transaction.

A notable example of this major impediment resulted in a hard fork[67] of one the most popular blockchains, Ethereum, in 2016. The hack of the DAO, the first notable attempt at a decentralised autonomous organisation operating an investment fund, resulted in the loss of millions in crypto assets which, in principle, could not be recovered without a change of heart from the hacker. Faced with an event of such unprecedented scale, to restore the situation, it was decided to perform a retroactive hard fork. As a result, the hack exists on the initial version of the Ethereum blockchain, now referred to as Ethereum classic, but does not exist on the new fork, which was initiated at a block preceding the one containing the transaction embodying the contested transfer of funds.

This problem may further exist even where pseudonymity is not the issue at stake. If the transaction involves funds held on a non-custodian wallet, there is no possibility of forced execution should the person refuse to proceed with the reverse transaction. The very nature and functionality of distributed ledgers prevent it, and in the absence of any centralised intermediary with the power of disposal over the funds, not much can be done.

Certainly, it can alternatively be relied on indemnities or execution by equivalent. These do yet provide merely partial satisfaction in most cases. If losing 1'000 USDC can be compensated by $1'000 (because the USDC is a stablecoin of which each unit corresponds to $1), losing 1'000 BTC can hardly be compensated by the corresponding value at a fixed moment in time, as such value fluctuates and could have been much higher (or lower) at another moment. Any fixed compensation will in such case entail a potential loss. Similarly, losing crypto assets being governance tokens allowing one to vote in the context of a decentralised autonomous organization is only partially compensated with a sum paid out in a fiat currency. Such a sum will not necessarily allow reinstating the lost voting power.

67 A hard fork is the result of the implementation in the blockchain's code of new rules incompatible with the previous code. Nodes which do not update cannot communicate with those which have updated. If both categories of nodes continue to pursue their activity, two cognate networks are maintained. For example, Bitcoin Cash is the result of a hard fork of the Bitcoin blockchain.

6 Conclusion

None of the hurdles and impossibilities listed in this contribution is to be understood as absolute. Advances in technology and regulatory amendments may provide solutions to many of them. Resolving issues triggered by pseudonymity while preserving the advantages and spirit of distributed ledgers requires a refinement of the problem. Thus, to enable helpful findings, it is necessary to steer research towards the problematic areas. This is precisely what this contribution intends to do.

Considering the presented developments, PIL appears partially ill-fitted in distributed ledger contexts.

Firstly, it is mostly ill-equipped to deal with fully decentralised transactions rather than all transactions occurring in a distributed ledger environment. This is particularly because, with respect to such transactions, parties generally make no choice regarding the applicable law. As a result of the principles applicable when determining the applicable law in the absence of a choice, pseudonymity becomes a particularly important stumbling block, with, for now, few existing alternatives to mitigate it. Research should therefore specifically focus thereon.

Secondly, debating and improving PIL is relevant to the extent that the outcome of judicial procedures can be enforced. The applicable law and jurisdiction hardly matter if it is known from the outset that the decision will never be implemented, or will only result in partial satisfaction. The latter fact may be a far greater crux in the case.

PART 2

Blockchain Assets and Conflict of Laws: General Issues

CHAPTER 7

Taxonomy and Characterisation of Crypto Assets in Private International Law

Felix Krysa

1 Introduction

Crypto assets are on everyone's lips and are increasingly becoming an economically relevant phenomenon. While the combined market capitalisation of all crypto assets was still "just" under 25 billion US dollars in March 2017, it increased to around 1.6 trillion US dollars in August 2021. During this time, the trading volume within 24 hours has climbed from 900 million US dollars to 80 billion US dollars.[1] Although crypto assets have become a relevant economic factor, the legal treatment of this topic is still in its infancy, both on the national and the international level. For starters, the term crypto asset is as miscellaneous as it is unspecific, not only in the legal sense but also in the scientific debate. On the Ethereum blockchain alone, there are already more than 400,000 contracts allowing tokens to be issued that comply with the ERC-20 standard,[2] and that have a wide variety of functions. The crypto assets created in this way differ considerably from one another in terms of their economic significance, their mode of operation, and their dynamics.

When it comes to Private International Law (PIL) and crypto assets, the first question to be answered is which crypto assets exactly are relevant. Due to the large number of crypto assets that already exist, and those that can be expected to still be created, the individual examination of crypto assets would neither be possible nor useful. Any systematic treatment of crypto assets, however, first presupposes that a uniform assessment is possible at all. In view of the different designs of the multitude of crypto assets, it is difficult to make general statements regarding their treatment. Therefore, it is first necessary to order and group the crypto assets by means of various criteria relevant for the respective purpose in order to be able to discern the groups that are meant. Such a procedure, in which objects are classified according to certain criteria

1 *Cf.* "Global Cryptocurrency Charts: Total Cryptocurrency Market Cap" (*CoinMarketCap*) <https://coinmarketcap.com/charts/> accessed 30 June 2023.

2 "Token Tracker" (*Etherscan*) < https://etherscan.io/tokens> accessed 30 June 2023.

© FELIX KRYSA, 2023 | DOI:10.1163/9789004514850_009
This is an open access chapter distributed under the terms of the CC BY-NC-ND 4.0 license.

by means of a uniform procedure or model, *i.e.*, classified into categories or classes, is called taxonomy.[3]

If it is already difficult to make specific statements on crypto assets in general, this is all the more true for legal issues and especially for PIL. To be able to answer the question of which law is applicable to a situation that involves crypto assets and legal questions, it must first be determined which provisions of PIL decide on the law applicable to the situation. In accordance with the typical structure of conflict-of-laws rules,[4] the determination of the applicable law requires a legal category to which the rule applies and a connecting factor, *i.e.*, a factual element that identifies the state whose law applies. These legal categories are concepts not tailored to specific crypto assets and require subsumption. If the applicable law is to be determined for matters relating to crypto assets, the question always arises in which legal category the respective crypto asset is to be put, *i.e.*, how it is to be characterised. To make a general statement in this respect, a taxonomy adapted to PIL is required which is oriented towards the differentiation criteria of PIL. While a taxonomy systematises from a purely factual perspective and allows an orderly classification under individual legal categories, the use of legal categories in conflict-of-laws provisions also serves the structured overview, albeit from a legal perspective.[5] Hence, characterisation has the task of reconciling the classification from both an actual perspective and a legal perspective. In contrast, a taxonomy adapted to PIL is a prerequisite for a systematic treatment of the determination of the law applicable to crypto assets.

3 Wolfgang J. Koschnik, "Taxonomie," in *Standard dictionary of the social sciences. Volume 2, Part 2 M-Z. German-English* (München: K.G. Saur 1993); CryptoCompare, *CryptoassetTaxonomy Report* (2018), 14 <https://www.cryptocompare.com/media/34478555/cryptocompare-cryptoasset-taxonomy-report-2018.pdf> accessed 30 June 2023.

4 See, on the structure of conflict-of-laws rules, exhaustively Jürgen Basedow, "Choice of Law," in Jürgen Basedow, Giesela Rühl, and Pedro De Miguel Asensio (eds), *Encyclopedia of Private International Law* (Edward Elgar 2017), 312, 313–317.

5 Under Schurig's bundling theory, this feature of conflict-of-laws rules is referred to as vertical bundling; see on Schurig's "Bundling Theory," Gerald Mäsch, "Preliminary Question," in Stefan Leible (ed), *General Principles of European Private International Law* (Wolters Kluwer 2016), § 6.02.

2 Taxonomy of Crypto Assets

If an in-depth treatment of crypto assets requires precise language and terminology,[6] which is established through classification into different categories, the question first arises as to which criteria should be used to classify crypto assets. Any classification also serves to deal more sensibly with the design, application, and regulation of tokens.[7] To this extent, various criteria are used to classify crypto assets based on their properties. However, due to the large number of properties that can be used,[8] a uniform system for categorising crypto assets has not yet been established.[9] Even if there is agreement on the property that is to be used for differentiation, the categorisation based on these properties differs in part from one another[10] or changes over time.[11] In the following, it will first be examined which properties all crypto assets have in common and thus which are ruled out for a differentiation between the various crypto assets. At the same time, these common properties allow the creation of a basis for a general definition of crypto assets. Subsequently, various criteria that can be used to classify crypto assets will be presented. In a third step, it will be examined which of these properties are suitable differentiation criteria for PIL.

2.1 *Common Characteristics of Crypto Assets*

To be able to determine which properties can be used to categorise crypto assets, it is first necessary to examine the properties common to all crypto assets. These properties are unsuitable from the outset to serve as differentiating criteria. At the same time, the compilation of the common properties allows distinguishing the object of analysis from other phenomena that are outside of the analysis' scope.

---

6 Shermin Voshmgir, *Token Economy: How the Web3 reinvents the Internet* (2nd ed, Shermin Voshmgir, BlockchainHub Berlin 2020), 210; Valeria Ferrari, "The regulation of crypto-assets in the EU – investment and payment tokens under the radar" (2020) 27 Maastricht Journal of European and Comparative Law 325, 329.

7 Voshmgir (n 6), 213.

8 CryptoCompare (n 3).

9 Luis Oliveira et al., "To Token or not to Token: Tools for Understanding Blockchain Tokens," 5 <https://www.zora.uzh.ch/id/eprint/157908/1/To%20Token%20or%20not%20to%20Token_%20Tools%20for%20Understanding%20Blockchain%20Toke.pdf> accessed 30 June 2023.

10 *Id*.

11 CryptoCompare (n 3), 36.

There is general agreement of the fact of a crypto asset being an asset created or transferred on a blockchain network using cryptography.[12] An asset is a right or any reference object of an economic value.[13] This implies, firstly, the concept of crypto assets being very broad and covering a wide range of real-world phenomena. Secondly, it also becomes clear how blurred the concept is due to the large number of phenomena covered. For the present analysis, one implication is to draw on a wide range of criteria for a taxonomy of crypto assets. This also shows the difference between the category "crypto assets" and the category "digital assets". Contrary to the latter, the former is necessarily based on the use of a blockchain. Conversely, this indicates that a taxonomy of crypto assets cannot be based on the fact of using blockchain technology.

2.2 *Possible Criteria for a Taxonomy of Crypto Assets*

Although the blockchain and crypto assets are still in their early stages, numerous approaches have already emerged to categorise crypto assets. The methods developed so far differ in their perspective and in the level of detail with which a differentiation is made. Economic, technical, or functional criteria are used for differentiation.[14] With regard to the level of detail, the spectrum ranges from taxonomies working with only one distinguishing criterion, to others using up to eleven different criteria to distinguish crypto assets.

Some authors differentiate crypto assets based on functionality into currency-like and investment-like tokens.[15] Another widely used distinction, especially in the legal analysis on crypto assets,[16] follows this functional distinction as a starting point, but differentiates between payment, utility, and

12 Ferrari (n 6), 326; Daniel T. Stabile, Kimberly A. Prior and Andrew M. Hinkes, *Digital Assets and Blockchain Technology* (Edward Elgar 2020), 25.

13 The Oxford English Dictionary defines an asset as, *inter alia*, an item of value owned, see "asset, *n.*," *Oxford English Dictionary* (September 2021) <https://www.oed.com/view/Entry/11866> accessed 3 September 2021. However, a restriction to such objects that have an economic value would fail to recognise in a legal analysis of crypto assets that the law also grants rights to such objects that have no economic value at all.

14 Also emphasising the lack of a uniform taxonomy from a legal perspective, European Banking Authority, *Report with advice for the European Commission: on crypto assets*, 7 (*EBA*, 9 January 2019) https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2545547/67493daa-85a8-4429-aa91-e9a5ed880684/EBA%20Report%20on%20crypto%20assets.pdf?retry=1 accessed 30 June 2023; Oliveira et al. (n 9), 5; Ferrari (n 6), 329.

15 Iris M. Barsan, "Legal Challenges of Initial Coin Offerings (ICO)" (2017) Revue Trimestrielle de Droit Financier 54, 56 *et seq*.

16 Filippo Annunziata, "Speak, If You Can: What Are You? An Alternative Approach to the Qualification of Tokens and Initial Coin Offerings" (2020) European Company and Financial Law Review 129, 136.

investment tokens.[17] However, the distinction between these three categories is not uniform and the terminology used varies. Legislators and authorities, who are guided by this functional demarcation, diverge markedly when it comes to the meaning of the three categories.[18] One very broad definition describes payment tokens as a means of exchange, utility tokens as a means of gaining access to something to be used, and investment tokens as a means of investing and raising capital.[19] According to another view, a payment token is defined by the three economic functions of a currency, *i.e.*, the role as a medium of exchange, a store of value and a unit of account.[20] According to this view, a utility token is understood as a token which does not serve as a means of payment or exchange. Finally, an investment token is thought to resemble a financial instrument, such as a share or bond. The classification as an investment token is further made dependent on whether the token embodies a value outside the blockchain, since otherwise it would be a utility token.[21] Others differentiate according to whether the respective token grants rights. Following this approach, a payment token does not grant a right but, because of its exclusive allocation and the sometimes limited number of units, is a means of exchange or serves investment purposes or the storage of value. Investment tokens are characterised by the fact that they grant rights. Utility tokens

17 Mirjam Egger, "Was ist ein Token? Eine privatrechtliche Auslegeordnung" (2018) Aktuelle Juristische Praxis 558, 561; Philipp Hacker and Chris Thomale, "Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law" (2018) European Company and Financial Law Review 645, 649; similar Dirk A. Zetzsche et al., "The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators" (2019) 60 Harv. Int'l L.J. 267, 276; Philipp Maume and Mathias Fromberger, "Regulation of Initial Coin Offerings: Reconciling U.S. and E.U. Securities Laws" (2019) 19 Chicago Journal of International Law 548, 558; Chris Brunner, "Introduction," in Chris Brummer (ed), *Cryptoassets: Legal, Regulatory, and Monetary Perspectives* (Oxford University Press 2019), 2; see also ESMA's Advice on Initial Coin Offerings and Crypto-Assets from 9 January 2019, which distinguishes between payment-like, utility-type and investment-type cryptoassets, European Securities and Markets Authority, "Advice on Initial Coin Offerings and Crypto-Asset" (*ESMA*, 9 January 2019) <https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf> accessed 30 June 2023.

18 See for an overview of various European legislators and authorities thinkBLOCKtank, "Position paper on the regulation of tokens in Europe (version 1.0): Part C: National legal & regulatory frameworks in select European countries" (*thinkBLOCKtank*, June 2019) <https://distributed-ledger-consulting.de/wp-content/uploads/2019/08/thinkBLOCKtank-Token-Regulation-Paper-v1.0.pdf> accessed 30 June 2023.

19 Brunner (n 17), 2.

20 Sarah Green, "It's Virtual Money," in David Fox and Sarah Green (eds), *Cryptocurrencies in Public and Private Law* (Oxford University Press 2019), para. 2.01.

21 Annunziata (n 16), 137.

are said to enable access to a specific product or service, which is often provided via a DLT[22] platform, while not being accepted as a means of payment for other products or services and not necessary granting a right.[23] Another approach includes, under the category of payment tokens, those tokens that are intended to function as a means of payment for goods and services outside the platform, while utility tokens are understood to provide a functional benefit by giving access to a product that the token-issuing entity itself has created or is in the process of creating, and investment tokens are defined as a promise of future cash flows.[24]

A further approach also uses a functional consideration as the starting point, but the relevant categories are modelled on the legal categories of existing regulations. For example, security tokens are considered, under this approach, to be all tokens that can be regarded as financial instruments in the sense of EU regulation; cryptocurrency tokens are defined as payment instruments excluded from MiFID II; and utility tokens are understood as all tokens that are neither security nor cryptocurrency tokens.[25]

If a functional approach is taken, a distinction may also be made as to whether the issuer of the tokens originally assigns the respective function to these tokens or whether this function is subsequently assigned to them in commercial transactions.[26] After all, an unambiguously functional classification is not always possible. For example, Ether could be classified as a payment token since the token as such does not embody any claims, while it also serves to remunerate transactions on the Ethereum blockchain, thereby providing access to the Ethereum blockchain, and thus could be classified as a utility token as well.[27] According to a partially held view, the three categories of payment, utility, and investment token should therefore not be exclusive, and tokens can be assigned not to only one of the categories specified, but also to two or all three categories mentioned.[28] Others see the three categories as

22 DLT is the abbreviation for "Distributed Ledger Technology," the technology on which the blockchain is built.

23 European Banking Authority (n 14).

24 Hacker and Thomale (n 17), 652 *et seq*.

25 thinkBLOCKtank (n 18), 13 *et seq*.

26 Annunziata (n 16), 137.

27 See on the one hand Maume and Fromberger (n 17), 550 and Hacker and Thomale (n 17), 652, who refer to Ether as a cryptocurrency; and on the other hand CryptoCompare (n 3), 30, who categorise Ether as a utility token; see also European Banking Authority (n 14), 7.

28 Ferrari (n 6), 329; thinkBLOCKtank (n 18), 13; Swiss Financial Market Supervisory Authority (FINMA), "Guidelines for enquiries regarding the regulatory framework for initial

merely archetypes, with each token sharing some or all of the types to some extent.[29]

From a legal perspective, a distinction is made as to whether a token is subject to claims that can be enforced outside the blockchain. If this is the case, it is a "native" token, otherwise it is a "non-native" token.[30] Similarly, a distinction could be made as to whether the token generally embodies a value that exists outside the blockchain. If this is the case, it is an "extrinsic" token, otherwise it is an "intrinsic" token.[31] Therefore, the distinction between "extrinsic" and "intrinsic" or "native" and "non-native" is based solely on the object represented outside the blockchain. The classification as non-native requires the token to represent a claim, whereas an extrinsic token already exists if the token only represents any value outside the blockchain. The extrinsic tokens are sometimes also referred to as "asset-backed," non-native tokens as "coloured coins", and intrinsic tokens as "native tokens".[32] Another approach for classification aims to combine the functional distinction between currency, utility, and investment tokens with the representation of claims that are enforceable outside the blockchain.[33]

From a technical point of view, tokens can be categorised according to the level at which they are located in the blockchain network. In this regard, a

---

coin offerings (ICOs)" (*FINMA*, 16 February 2018), 3 <https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?la=en> accessed 30 June 2023.

29 Hacker and Thomale (n 17), 652.

30 Egger (n 17), 559; Jonathan Rohr and Aaron Wright, "Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets" (2019) 70 Hastings Law Journal 463, 469 *et seq*. also use the distinction between the protocol and application level as a starting point, but for the application level they additionally distinguish between utility and investment tokens on the basis of the functionality of the tokens, see on this already above.

31 Christiane Wendehorst, "Digitalgüter im Internationalen Privatrecht" (2020) Praxis des Internationalen Privat- und Verfahrensrechts 490, 494–495.

32 Hans Caspar von der Crone, Franz J. Kessler, and Luca Angstmann, "Token in der Blockchain – privatrechtliche Aspekte der Distributed Ledger Technologie" (2018) 114 Schweizerische Juristen-Zeitung 337, 338; Samuel Zogg, "Bitcoin als Rechtsobjekt – eine zivilrechtliche Einordnung" (2019) Zeitschrift für juristische Weiterbildung und Praxis 2019, 95.

33 Pierluigi Freni, Enrico Ferro, and Roberto Moncada, "Tokenization and Blockchain Tokens Classification: a morphological framework," 2 <https://ieeexplore.ieee.org/document/9219709> accessed 30 June 2023.

distinction can be made between protocol tokens and second-layer tokens.[34] Protocol tokens are the original unit of account of the respective blockchain network, on which the respective blockchain protocol is based, and by means of which, for example, the transaction costs are also settled; second-layer tokens, in contrast, are those tokens that are implemented on the respective blockchain by means of a smart contract.[35] Another technical criterion that can be used for the categorisation of tokens is their fungibility: Depending on the technical design of the blockchain and the token, the latter can be uniquely identifiable or merely a quantifiable value (so-called fungibility).[36] From a technical perspective, it is also relevant whether fragments of tokens can exist and whether there can be more than one token.[37]

From a purely business perspective, a distinction can be made as to whether the tokens are issued in return for a counter-performance.[38] From an economics perspective, one could further differentiate according to the areas of the economy in which the respective blockchain networks are used.[39]

Others pursue a comprehensive approach for the categorisation of tokens and want to link the categorisation of a crypto asset to several properties. According to one approach, for example, the categorisation should consider, among other things, the technical basis, fungibility, transferability, durability, incentives and supply, value stability, privacy, legal and regulatory classification, and exchangeability.[40] The very different characteristics of the tokens, however, result in a large number of potentially various criteria to be

34 Egger (n 17), 559; sometimes protocol tokens are referred to as native tokens and second-layer tokens are referred to as non-native tokens; for the purposes of this contribution, however, the property "native", as described above, is supposed to provide information on whether the crypto asset represents a value located outside the blockchain.

35 One case are multi-asset ledger tokens, which are issued directly on the blockchain like protocol tokens, but which have no function for the respective blockchain protocol itself; see Voshmgir (n 6), 426.

36 Oliveira et al. (n 9), 7.

37 Voshmgir (n 6), 227.

38 Zetzsche et al. (n 17), 279.

39 CryptoCompare (n 3), 21.

40 Voshmgir (n 6), 242; a comprehensive approach is also taken by Thomas Euler, "The Token Classification Framework: A multi-dimensional tool for understanding and classifying crypto tokens" (*Untitled Inc*, 18 January 2018) <http://www.untitled-inc.com/the-token-classification-framework-a-multi-dimensional-tool-for-understanding-and-classifying-crypto-tokens/> accessed 30 June 2023 and InterWork Alliance Inc., "Token Taxonomy Framework (TFF) – January 2022" (*GitHub*, January 2022) <https://github.com/InterWorkAlliance/TokenTaxonomyFramework/blob/main/token-taxonomy.md> accessed 30 June 2023.

identified, which result in a variety of possible combinations. A categorisation based on a holistic approach is therefore only possible to a limited extent due to the multitude of possible combinations and is also not meaningful. If a taxonomy is to enable a systematic consideration through grouping, this presupposes that the differentiation criteria used allow for a corresponding grouping quantitatively and qualitatively. This is not the case with such a holistic approach.

2.3 *A Taxonomy of Crypto Assets for PIL*

The preceding overview shows that the search for an all-encompassing taxonomy of crypto assets is neither possible nor desirable. A comprehensive taxonomy would require the consideration of a multitude of different criteria; it would be very complex and would not simplify a systematic analysis of crypto assets. At the same time, such a taxonomy would also be overloaded since most of the criteria mentioned have no effect on the legal assessment. Rather, a taxonomy, if it is to be beneficial for the conflict-of-laws analysis, must be oriented towards those properties that are of relevance under conflict-of-laws rules and be limited to a few distinguishing criteria. This ensures, firstly, the possibility of a systematic examination of the conflict-of-laws aspects of crypto assets; secondly, simplifies the process of categorisation; and thirdly, minimises the potential for qualification errors. It follows from the variety of different taxonomies that there is not one taxonomy that should form the basis of any systematic analysis of crypto assets, but that the suitability of a taxonomy of crypto assets always also depends on the particular field of application, and that the suitability is also influenced within a field of application by the respective specific purpose of use. In this context, it follows from the restriction to questions of conflict of laws that the different criteria which can be derived from an economic view are of minor importance for a taxonomy for conflict-of-laws purposes.

Thus, the goal of a taxonomy adapted to conflict of laws should be to first use few delimitation criteria, to adapt these delimitation criteria to conflict of laws, and to ensure a legally uniform assessment of the groups formed in this way. The latter, however, does not presuppose the correspondence of the groups to the constituent elements of the individual conflict-of-laws rules. On the one hand, the connecting factors used in PIL are very broad and regularly cover a multitude of cases.[41] On the other hand, the

41 For example, Article 4(1)(a) and (b) of the Rome I Regulation refer generally to the existence of a contract of sale or a contract for the provision of services, whereas Article 4(1)(c) to (h) of the Rome I Regulation contain different connecting factors for specific

determination of the applicable law is based on the search for the closest connection of the facts to a legal system, so that – irrespective of the specification of the respective provision in the particular case – PIL often follows uniform principles.[42] However, there is much to be said for following an already existing taxonomy at the price of a partially non-uniform classification. In particular, such a taxonomy enables a holistic view of different categories of tokens under different aspects.

Regarding the delimitation criteria to be used, those are to be considered for a taxonomy of crypto assets for the purposes of conflict of laws, which allow for a functional delimitation. The law is regularly largely technology neutral. Thus, the specific technical design of a blockchain generally has no influence on the legal assessment. Consequently, a taxonomy based on technical differentiation criteria would not benefit a generalising legal assessment of tokens. Therefore, a delimitation based on technical differentiation criteria is not useful. However, an exception applies for the question of whether a crypto asset is fungible, *i.e.*, unique. The uniqueness of a crypto asset allows the unambiguous and definite attribution of a crypto asset to a right or object existing outside the blockchain. Such an unambiguous attribution and the uniqueness of a non-fungible crypto asset may require a different legal characterisation. The fungibility thus represents a potentially legally relevant distinguishing criterion. This distinguishing criterion must be considered when classifying crypto assets for the purpose of handling crypto assets legally.

When categorising an individual crypto asset, the function of the crypto asset might additionally be of importance, as the legal classification is possibly decisively linked to the function of the token. As already mentioned, in the legal consideration of crypto assets, a distinction based on the function of the crypto asset is regularly emphasised, and a subdivision into currency, utility, and investment tokens is made. At least for the assessment under conflict of laws, such a distinction is – as will be seen – largely superfluous. A distinction based on the function of crypto assets is at most relevant for the question of the regulatory classification of crypto assets, which has only a very subordinate significance for PIL. But even for regulatory purposes, a functional distinction is only of limited use. The mere function of a crypto asset

---

contractual objects or circumstances in which the contract is concluded. See Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I)," [2008] OJ L 177/6 (hereafter "Rome I Regulation").

42 Ulrich Magnus, "Art 4 Rome I" in Ulrich Magnus and Peter Mankowski (eds), *European Commentaries on Private International Law Volume II Rome I Regulation* (Otto Schmidt 2016), para. 22.

can only be used to a limited extent to determine the regulatory requirements to which the respective crypto asset is subject.[43] If the function of the crypto asset is of subordinate significance for the legal categorisation, such a differentiation would only be meaningful at best in the sense of a uniform taxonomy for the legal analysis of crypto assets. An argument against an additional differentiation based on the function of the crypto asset is, however, a complication in the legal assessment of crypto assets by always requiring an additional differentiation criterion. Further, this additional criterion possibly obscures and overlays the criteria that have an impact on the legal characterisation.

If one weighs the abovementioned disadvantages of an additional differentiation between the various functions of crypto assets and their previously mentioned advantages, there is a strong case for dispensing with this differentiation and leaving it at a two-tier distinction between fungible and non-fungible crypto assets and native and non-native crypto assets, at least for the purposes of PIL. First, a distinction must be made as to whether the crypto asset itself is unique due to its technical design (fungible or non-fungible crypto asset). In a second step, it is necessary to distinguish whether the crypto asset is an object of representation, *i.e.*, whether it embodies a right (non-native crypto asset) or whether its function is limited to the quantitative assignment of a value to a public key on the blockchain (native crypto asset).

The taxonomy of crypto assets proposed here deviates to a considerable extent from the taxonomy previously used as a basis in the legal examination of crypto assets. However, such a deviation can be justified for PIL by the fact that the taxonomy regularly used so far does not sufficiently consider the special characteristics and categories of conflict of laws. The distinction between the functions of crypto assets has created the danger of ambiguities due to differing designs of the individual categories and the different standards used as a starting point. It could not benefit the systemisation of the treatment of crypto assets under conflict of laws. Although the taxonomy proposed here can be criticised as being overly simplistic, it allows a clear and unambiguous classification into one of the four possible categories which result from the two distinguishing criteria of fungibility and representation of assets located outside the blockchain. Usually, this allows for a uniform treatment of the respective category under conflict of laws. The taxonomy proposed here also has the advantage of being independent of subjective elements and therefore allowing an unambiguous classification. For the classification, it is

43 See also on this *infra* section 3.2.5.

not important whether the corresponding function of the crypto asset was intended by its issuer. The only decisive factor is which function the respective crypto asset actually has in commerce, as it is only the actual use of the crypto asset that matters for the legal classification.

Overall, however, it must be noted that recourse to a taxonomy cannot replace the examination of which regulations apply to the respective crypto asset in each individual case. In this respect, a "substance over form approach" is required.[44] A taxonomy allows different types of crypto assets to be grouped together and to make generalising statements in this respect. However, it does not relieve from examination whether the respective crypto asset can be subsumed under the connecting factor of the individual conflict-of-laws rule.

3 Characterisation of Crypto Assets

Crypto assets can be divided into the four categories depending on the criteria of fungibility and representation. This raises the question of how crypto assets categorised in this way are to be treated legally. It is a question of subsuming the previously formed groups under the existing conflict-of-laws rules. In PIL, this process is referred to as classification, characterisation or qualification.[45]

3.1 *What is Characterisation?*

Through characterisation, it is decided whether a legal question[46] arising from a factual situation can be shoehorned into the scope of a conflict-of-laws rule.[47] Sometimes the respective conflict-of-laws rule is used as a starting point; in other words, it is asked which legal questions are covered by the conflicts rule, *i.e.*, how the legal categories of the respective conflict-of-laws rule are to

44 Ferrari (n 6), 326.

45 Lord Collins of Mapesbury and Jonathan Harris (eds), *Dicey, Morris & Collins on the Conflict of Laws* (15th edn, Sweet & Maxwell 2018), vol. 1, para. 2-001; Paul Torremans et al. (eds), *Cheshire, North & Fawcett Private International Law* (15th edn, Oxford University Press 2017), 42; see also Ernst G Lorenzen, "The Qualification, Classification, or Characterization Problem in the Conflict of Laws" (1941) 50 Yale L. J. 743.

46 Already the specific subject matter of the qualification is disputed; see Felix M. Wilke, *A Conceptual Analysis of European Private international Law* (Intersentia 2019), 113–114 with further references.

47 Christopher Forsyth, "Characterisation revisited: an essay in the theory and practice of the English conflict of laws" (1998) 114 L.Q.R. 141, 145–146; O. Kahn-Freund, *General Problems of Private International Law* (*Volume 143*) (Brill 1974) 139, 369 *et seq*.

be interpreted.[48] Regardless of whether one looks at the question from the perspective of the facts or the conflicts rule, the problem remains the same: the legal question arising from the respective facts must be reconciled with the concepts of the respective conflict-of-laws rules. In this process, both the nature of the legal question and the scope of application of the legal category must be examined and brought into harmony with one another. It is therefore a matter of interpreting the legal categories used on the factual side[49] and subsuming the legal question thereunder. For the characterisation of crypto assets, this means on the one hand that the characterisation of crypto assets under the conflict-of-laws rules is always subject to the individual case which cannot be considered schematically. On the other hand, a precise analysis of all actual circumstances is required in each case to characterise crypto assets.

Another distinction must be made between the characterisation and the determination of the scope of the individual governing law, as laid down, for example, in Article 12 of the Rome I Regulation[50] and Article 15 of the Rome II Regulation.[51] Both the characterisation and the determination of the scope of the individual governing law are concerned with the question of which legal issues are covered by the respective conflict-of-laws rule. However, the characterisation is to be carried out at the beginning of the determination of the applicable law and the determination of the scope of the governing law is at its end. If characterisation thus involves attributing legal questions arising from the facts of the case to individual conflict-of-laws rules, the scope of the governing law determines which substantive rules of the referred law apply to the facts of the case.

Characterisation is not a process that is special to the conflict of laws, but is a typical part of any legal operation.[52] Every application of a provision requires a step in which it is examined whether a fact or legal question is covered by a factual element of the respective provision.[53] This follows from the fact that

48 Lord Collins of Mapesbury and Harris (n 45), vol. 1, paras. 2-002-003.

49 See also explicitly K. Lipstein, *The General Principles of Private International Law* (*Volume 135*) (Brill 1972), 98, 198.

50 Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I) [2008] OJ L177/6.

51 Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II) [2007] OJ L199/40 (hereafter "Rome II Regulation").

52 Wilke (n 46), 115; Gilles Cuniberti, *Conflict of Laws: A Comparative Approach* (Edward Elgar 2017) 76.

53 Stefania Bariatti, "Classification (characterization)," *Encyclopedia of Private International Law* (Edward Elgar 2017), 357.

law operates by reference to abstract terms, which are based on a legal concept, and that it must be examined in detail for each factual element whether it is covered by the respective concept. This procedure is generally referred to as "subsumption." Characterisation is a special type of subsumption. It differs from subsumption in general in that, due to the normative structure of the rules of conflict of laws, its subject matter is generally not a purely factual question but a legal question arising from a factual situation. A necessary component of subsumption under the respective legal category is the formulation of the legal question arising from the facts in a way that allows the subsumption under the legal categories of the conflict-of-laws rules. For crypto assets, this first requires them to be clothed in a legal context before they can be subsumed under the legal categories of the conflict-of-laws rules. However, it must be ensured that the legal context is formulated as detached as possible from the substantive categories of the respective legal system to facilitate subsumption under the respective conflict-of-laws rule. The phrasing of corresponding legal questions is particularly difficult regarding crypto assets, as they are a comparatively young phenomenon whose legal categorisation still cannot be described as conclusively clarified. Also, the concept of crypto assets is rather complex and abstract, which makes the legal categorisation more difficult.

Therefore, if one wants to characterise crypto assets under conflict of laws, the first step is to determine the legal relationship resulting from the facts of the case from which the legal dispute has arisen. In the next step, it must be determined which conflict-of-laws rules are applicable to this legal relationship. Finally, it must be examined whether these conflict-of-laws rules also govern the legal relationship in question, to the extent that crypto assets are the legal object of this legal relationship.

So far, there are very few conflict-of-laws rules specifically tailored to crypto assets. Hence, crypto assets are regularly to be subsumed under the general conflict-of-laws rules. According to the preceding, as far as the applicability of the general conflict-of-laws rules to crypto assets is concerned, a distinction must be made: if, on the one hand, the legal category of a conflict-of-laws rule is formulated in general terms and detached from the specific object of the legal relationship,[54] crypto assets are not to be treated differently from other assets under the conflict-of-laws rules. A characterisation of the respective crypto asset is thus in principle not necessary for these conflict-of-laws rules. If, on the other hand, conflict-of-laws rules are linked to a particular object by

54 See *e.g.*, Article 4(1) of the Rome I Regulation, Article 4(1) of the Rome II Regulation.

defining the applicable law regarding a specific object,[55] it must be clarified whether and which crypto assets are covered by the respective object. Only in this respect a characterisation of the respective crypto asset is in fact required.

The question of the characterisation of specific crypto assets therefore becomes relevant if the conflict-of-laws rules determine the applicable law with recourse to a specific object. In addition, the legal nature of certain crypto assets is also of particular importance in determining the applicable law insofar as the holding of crypto assets is itself classified as a contractual or corporate relationship. Based on this assumption, the question also arises as to whether this legal relationship is to be qualified as a contract or a corporation within the meaning of the conflict-of-laws rules.

In the following, it will be examined in particular the legal categories typically used in conflict of laws, which at least partially refer to a legal object, and thereby elaborated whether crypto assets are legal objects in the sense of these legal categories. A characterisation, as a process including the interpretation of an individual conflict-of-laws rule, can only be done in relation to certain conflict-of-laws rules by virtue of the nature of the matter. The following remarks will refer to the conflict-of-laws rules of the EU. Insofar as there is a lack of unified regulations – especially in international property law – recourse will be made to the national conflict of laws of individual member states and potential commonalities will be examined.

3.2 *The Characterisation of Crypto Assets within Different Areas of PIL*

3.2.1 The Characterisation of Crypto Assets within Contractual Relations

Within contractual relationships, crypto assets may take on significance in four constellations. First, the holding of crypto assets itself can be understood as a contractual relationship in relation to other crypto asset holders or network participants (3.2.1.1); second, crypto assets themselves can be the subject of a contract (3.2.1.2). Third, the special circumstances of the acquisition of crypto assets may require a separate analysis under conflict of laws (3.2.1.3). Finally, contracts for the transfer of crypto assets also require special attention (3.2.1.4).

55 See, for example, Article 14 of the Rome I Regulation ("claim"), Article 3 of the GDPR, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L 119/1 (hereafter "GDPR") ("personal data"), also note international property law in the respective conflict-of-laws rules refers to the legal object thing to determine the applicable law.

3.2.1.1 *The Blockchain as a Contractual Relationship*

It has been argued that contractual relationships are established through the mere participation in a blockchain network.[56] Irrespective of whether one shares this legal assessment for substantive law, the question arises as to which conflict-of-laws rules determine the law applicable to such a potential contractual relationship.

The PIL of the European Union consists of the Brussels I*bis* Regulation[57] for determining the general competent court in cross-border disputes and the Rome I Regulation and Rome II Regulation for determining the law applicable to contractual and non-contractual obligations respectively. The existence of a contractual relationship between the participants in a blockchain network would influence the determination of the competent court as well as the applicable law. Regarding the competent court, besides the general jurisdiction according to Article 4 of the Brussels I*bis* Regulation, the special jurisdiction of Article 7(1) of the Brussels I*bis* Regulation on the place of performance of contracts would be available. The determination of the applicable law is governed by the Rome I Regulation if participation in a blockchain network is considered as giving rise to a contractual obligation within the meaning of Article 1(1) of the Rome I Regulation. In the absence of such a contractual obligation, the law applicable between the participants shall be determined by the Rome II Regulation.

It is partly assumed that the relationship between the participants in a blockchain network establishes a contractual obligation within the meaning of Article 1(1) of the Rome I Regulation[58] and thus also a contract within the meaning of Art 7(1)(a) of the Brussels I*bis* Regulation. The downloading and execution of the software is identified as the relevant voluntary conduct establishing the required contractual obligation.[59] However, there are both factual and legal reasons against the assumption of a contractual relationship or a contract within the meaning of the Brussels I*bis* Regulation and the Rome I Regulation. From a factual point of view, it is already questionable what exactly

56 See *e.g.*, Andrew Dickinson, "Cryptocurrencies and the Conflict of Laws," in David Fox and Sarah Green (eds), *Cryptocurrencies in Public and Private Law* (Oxford University Press 2019), para. 5.31 for the purposes of conflict of laws.

57 Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2012] OJ L351/1 (hereafter "Brussels I*bis* Regulation").

58 Paolo Bertoli, "Virtual Currencies and Private International Law" (2018) 54 Rivista di diritto internazionale privato e processuale 581, 599; regarding "cryptocurrencies," see Dickinson (n 56), para 5.31.

59 Dickinson (n 56), para. 5.27.

is to be considered as the voluntary conduct as giving rise to the contractual obligation.

In purely factual terms, three possible ways of participating in a network can be identified. First, participation is possible through the operation of a node, whereby the question of participation does not depend on the specific type of node.[60] Second, participation in a blockchain network could also take place by generating and announcing a key pair that conforms to a blockchain-specific address in terms of its format. Finally, participation could also be assumed if a contractual relationship is established with another person offering services related to the blockchain. An example of this is the creation of a user account at a crypto exchange.

However, from a factual perspective, none of these ways of participating in a blockchain network is suitable to establish a contractual obligation. For downloading and running the software of a blockchain network, this follows from the fact that neither is a necessary precondition for owning crypto assets. Crypto assets can be considered as being at the actual disposal of a person if this person generates a key pair and makes the public key known to the public. At the same time, the mere downloading and execution of the software does not lead to active participation in the network and neither does it necessarily involve the holding of crypto assets, nor do consensus or propagating activities always take place. It follows that downloading and executing the software of the blockchain network is neither a necessary nor a sufficient condition for participation in a blockchain network.

If both activities are not a prerequisite for participation in the blockchain network, active participation in the blockchain network cannot generally be inferred from them. If, instead, the creation of the key pair is taken as a starting point, this can take place completely separately from the blockchain network and is therefore also not suitable for establishing a contractual relationship with the participants of the blockchain network. No special software is required for generating the key pair: the private key is a random number within a certain number range and the public key is calculated by means of a mathematical equation.[61] Even if the public key is made known to the outside world, the person who created the key pair has no way of interacting with the network. This also applies if he is assigned tokens on the blockchain due to the public key being made public. He has no possibility of disposing of them due to the mere ownership of the private key. To do so, he must always make use of a node

60 On the different types of nodes within the Bitcoin network see Andreas M. Antonopoulos, *Mastering Bitcoin* (2nd edn, O'Reilly 2017), 172.

61 On this, see exhaustively *Id.*, 58, 60.

that propagates the transaction in the network. The mere creation of a key pair is thus also not suitable for establishing a contractual relationship. Finally, due to similar considerations, it cannot be assumed as a general rule that the conclusion of a contract with a person offering services on the blockchain creates a contract with the participants in the network themselves. The contractual relationship with the service provider is detached from the blockchain network and at most establishes contractual claims against the service provider.

On a legal level, it is questionable as to whether a voluntary obligation within the meaning of Article 1(1) of the Rome I Regulation and Article 7(1)(a) of the Brussel I*bis* Regulation can be assumed merely because of a participation within a blockchain network. A contractual obligation in this sense presupposes the existence of a relationship between the parties that has actually reached a stage where obligations have been voluntarily assumed by one party towards another.[62] Thus, a freely consented obligation is required.[63] This does not necessarily require a contract; a voluntary obligation through a unilateral declaration can also establish a contractual obligation within the meaning of Article 1(1) of the Rome I Regulation.[64] The importance of the voluntary obligation entered into for the application of the Rome I Regulation is not least illustrated by the exclusion of pre-contractual claims for damages from the scope of application of the Rome I Regulation.[65]

Accordingly, the concept of contract is interpreted broadly for the law of international jurisdiction.[66] This must also be taken into account for the interpretation of the term "contractual obligation" in Article 1(1) of the Rome I Regulation.[67] For the Brussels Convention, for example, it is assumed that a mere promise of profit constitutes a contract or claims arising out of a contract

62 Alfonso-Luis Calvo Caravaca and Javier Carrascosa González, "Art 1 Rome I," in Ulrich Magnus and Peter Mankowski (eds), *European Commentaries on Private International Law Volume II Rome I Regulation* (Otto Schmidt 2016), para 5; Michael McParland, *The Rome I Regulation on the Law Applicable to Contractual Obligations* (Oxford University Press 2015), Para. 6.15.

63 Caravaca and González (n 62), para. 5 *et seq*. with further references to the literature and the CJEU case law.

64 *Id*., para. 6.

65 McParland (n 62), para. 6.17.

66 CJEU Case C-27/02 *Petra Engler v Janus Versand GmbH* [2005] ECLI:EU:C:2005:33, para. 48, regarding Article 5(1) of the Brussels Convention (1968 Brussels Convention on jurisdiction and the enforcement of judgments in civil and commercial matters, [1968] OJ L299/32 (hereafter "Brussels Convention")).

67 Ulrich Magnus, "Introduction Rome I," in Ulrich Magnus and Peter Mankowski (eds), *European Commentaries on Private International Law Volume II Rome I Regulation* (Otto Schmidt 2016), para. 37.

within the meaning of Article 5(1) of the Brussels Convention.[68] The will to be bound by the obligation to the other party in the event of acceptance by the other party must have been clearly expressed by unconditionally agreeing to perform the promised service on request.[69] When determining the existence of a contractual obligation, one must consider that the requirement of a contractual obligation primarily serves to distinguish the Rome I Regulation from the Rome II Regulation[70] and Article 7(1) from Article 7(2) of the Brussels I*bis* Regulation. All obligations under private law in civil and commercial matters must be classified as either contractual or non-contractual; they cannot be both simultaneously or neither.[71] For the demarcation of contractual and non-contractual obligations, it follows that a distinction must be made as to whether the asserted claim is based on an obligation arising from the general principles of law for all, or whether the obligation was entered into voluntarily and formed by the will of the parties.[72] The question therefore arises, whether an obligation previously not existing between the parties, even latently, is to be created and realised, or whether the obligation is merely a pre-existing legal or judicial obligation and its effects.[73]

Based on these criteria, the participants of a blockchain network, regardless of whether they merely hold tokens transferred on the blockchain or act as operators of nodes, cannot be classified as parties to a contractual obligation or a contract according to Article 1(1) of the Rome I Regulation and Art 7(1) of the Brussels I*bis* Regulation. This follows from the fact that a will to be bound by one's commitment is not expressed by the participants. There are no further-reaching obligations between the participants in a blockchain network and such further-reaching obligations are not desired. Regardless of which specific activity is used on the factual level to justify a contractual obligation through participation in a blockchain network, none of these activities clearly

68 CJEU Case C-27/02 *Petra Engler v Janus Versand GmbH* [2005] ECLI:EU:C:2005:33, para. 53.

69 CJEU Case C-180/06 *Renate Ilsinger v Martin Dreschers* [2009] ECLI:EU:C:2009:303, para. 55.

70 McParland (n 62), para. 6.09.

71 *Id.*, para. 3.10; Ulrich Magnus, "Introduction," in Ulrich Magnus and Peter Mankowski (eds), *European Commentaries on Private International Law Volume II Rome I Regulation* (Otto Schmidt 2016), para. 32; Jan D. Lüttringhaus, "Article 1," in Franco Ferrari (ed), *Concise Commentary on the Rome I Regulation* (2nd edn, Cambridge University Press 2020), paras. 10, 12, 18; Matthias Weller, "Art 1 Rome I Regulation," in Gralf-Peter Calliess and Moritz Renner (eds), *Rome Regulations* (3rd edn, Wolters Kluwer 2020), para. 2.

72 McParland (n 62), paras. 3.12, 6.40.

73 Ulrich Magnus, "Art 1 Rom I-VO," in Ulrich Magnus (ed), *J. von Staudingers Kommentar zum Bürgerlichen Gesetzbuch: Internationales Vertragsrecht I* (Sellier/de Gruyter 2016), para. 33.

expresses the intention to be bound by an obligation in the event of acceptance by the other party. This is already evident from the absence of an explicit declaration of intent in each of these activities.

Furthermore, an undetermined number of people regularly participate in the blockchain network and their identities are unknown. An intention of the participants in a blockchain network to establish rights and obligations by one of the aforementioned activities vis-à-vis the other participants, who are unknown to them and of whom there are regularly many, cannot be assumed. Otherwise, participation in a blockchain network would entail unforeseeable liability risks for participants in both quantitative and qualitative terms. However, even if one considers the type of claims participants in a blockchain network will invoke to enforce their rights, this argues against the assumption of a contractual obligation or contract. Claims against the other participants of the blockchain network are not directed at the provision of a service or a good, but are merely intended to prevent unlawful interference with the token and thus with the assets of the participant. The refraining from unlawful interference with the legal interests of someone else, though, is a legal obligation that may or may not exist independently of a voluntary obligation. Taking this delimitation criterion into account, participation in a blockchain network does not establish a contractual obligation or a contract.

In this respect, it must also be taken into account that the participants in the blockchain network do not suffer any disadvantage by the nonapplicability of the Rome I Regulation and Article 7(1) of the Brussels I*bis* Regulation. In this case, the special international jurisdiction is simply determined according to Article 7(2) of the Brussels I*bis* Regulation and the applicable law according to the Rome II Regulation. The rejection of the existence of a contractual obligation or a contract therefore does not deprive the participant of the blockchain network of a special place of jurisdiction or a determination of an applicable law. Also, even those authors who consider the Rome I Regulation to be applicable to these cases do not claim that rights and obligations would be always created between the participants in the blockchain network at the level of the substantive law solely due to their participation.[74] Thus, the Rome I Regulation has regularly no relevance for determining the legal effects of the relationship between the participants in the blockchain network, who have no further relationship with each other. Hence, the assumption of a contractual obligation or a contract between the participants of a blockchain network loses any significance also for conflict of laws.

74 Dickinson (n 56), para. 5.31.

Therefore, the relationship between the participants in a blockchain network is not to be classified as a contractual obligation within the meaning of Article 1(1) of the Rome I Regulation and Article 7(1)(a) of the Brussels I*bis* Regulation. The law applicable to the relationship between the participants is therefore not determined by means of the Rome I Regulation. However, this does not preclude the characterisation of the relationship between the participants in a blockchain network as a relationship under company law, for which one might argue. If this view were to be followed, the law applicable to this relationship would be determined by means of international company law.

If the entirety of the owners of a key pair were to be classified as a company, Article 24(2) of the Brussels I*bis* Regulation would provide an exclusive jurisdiction. In addition, there would be special rules on the determination of domicile in Article 63 of the Brussels I*bis* Regulation. Regarding the applicable law, unlike the international law of obligations, international company law has not yet been unified at the European level. In this respect, Articles 1(2)(f)-(g) of the Rome I Regulation explicitly excludes questions of company law from the scope of application of the Rome I Regulation. Thus, this provision presupposes the existence of the concept of "company" within the meaning of the Rome I Regulation. Even though the Rome I Regulation itself does not contain a definition of an "undertaking", the term is understood very broadly.[75] Accordingly, a company in this sense is any entity with an independent legal identity separate from individual membership.[76] This includes all forms of legal persons, all forms of partnerships or equivalent, and unincorporated membership clubs and associations that have legal personality.[77] However, this does not preclude national legislatures from defining the concept of a company more broadly, or more narrowly, for its respective conflict-of-laws rules. Thus, as a starting point and independently of the characterisation under the Rome I Regulation, the classification of a blockchain network as a company by a national conflict-of-laws rule is not excluded.

However, there are practical reasons against the classification of a blockchain network as a company. A mere blockchain network will regularly lack a structure that could be described as a company in the legal sense: Indeed, the network follows a programme code providing rules regarding the blockchain.

---

75 Peter Mankowski, "Art 1 Rome II," in Ulrich Magnus and Peter Mankowski (eds), *European Commentaries on Private International Law Volume III Rome II Regulation* (Otto Schmidt 2019), para. 130; Mario Guiliano and Paul Lagarde, "Report on the Convention on the law applicable to contractual obligations" (1980) 266 Official Journal C 282 1, Art. 1 para. 6 and Weller (n 71), para. 35 emphasise the flexibility of the concept of company.

76 McParland (n 62), para. 7.140.

77 McParland (n 62), para. 7.140.

This programme code could be understood as the basis of an agreement regulating the organisation of the company. However, the fact that the mere participants of a blockchain network who do not have any further tasks in the blockchain network beyond the ownership of crypto assets do not have a common purpose and, in particular, are not involved in the updating of the blockchain, speaks against a classification as a company. In this respect, it is also doubtful with which act exactly the participant of a blockchain network joins the company. Is the mere creation of a key pair sufficient? Does the key pair have to be attributed to a crypto asset? Finally, as is also the case for the existence of a contractual obligation within the meaning of Article 1(1) of the Rome I Regulation and Article 7(1) of the Brussels I*bis* Regulation, the question arises as to whether the participants in a blockchain network are willing to assume the obligations associated with the participation in a company. This is all the more true as participation is possibly anonymous and the number of participants in a blockchain network is often unknown. These arguments speak in favour of fundamentally rejecting the classification of a blockchain network as a company under conflict of laws in the absence of evidence to the contrary.

In addition, there might also be legal reasons for why a blockchain network should not be classified as a company at least within the meaning of the Rome I Regulation. In part, it is argued in favour of a more restrictive understanding of the concept of a company, which should exclude companies recognised under national law whose sole purpose is to regulate the relationships between the shareholders without the company interacting with the public.[78] However, the blockchain network itself does not regularly interact with the public. As already mentioned, the only common goal of the participants in the blockchain network is usually the operation of the network and the use of the network as such. Insofar as additional activities are undertaken – for example, in the context of a DAO – in which there is interaction with persons outside the network, these are activities for which participation in the blockchain network is a necessary condition, but which are otherwise completely detached from it. The respective organisations thus use the structures of the blockchain, but for them the blockchain is merely a means of decision-making. As such, any corporate structures modelled on the blockchain are therefore to be considered separately from the blockchain network.

78 Lüttringhaus (n 71), para. 80.

3.2.1.2 *Crypto Assets as Subject Matter of the Contract and Remuneration*

The mere participation in a blockchain network can thus neither lead to a contractual obligation nor the participation in a company under PIL. However, the PIL applicable to contractual obligations could be relevant to crypto assets insofar as crypto assets are the subject of a contract covered by the Brussels I*bis* and the Rome I Regulation.

The applicability of the Rome I Regulation is not excluded *a priori* by the fact of crypto assets being the subject matter of the contract. Neither in the Brussels I*bis* nor in the Rome I Regulation is the scope of application restricted to certain contractual subjects. Article 1 of the Rome I Regulation does not distinguish between different subject matters of a contract for the scope of application of the Rome I Regulation. Nor is the application of the Rome I Regulation for contracts on crypto assets excluded by Article 1(2) of the Rome I Regulation; in particular, Article 1(2)(d) of the Rome I Regulation is not applicable to these contracts. Even if crypto assets are to be classified as securities under conflict-of-laws rules in individual cases (see 3.2.5), contracts having crypto assets as their subject matter do not constitute "obligations arising under [...] other negotiable instruments" that "arise out of their negotiable character" as required for Article 1(2)(d) of the Rome I Regulation.[79]

When the law applicable to contracts involving crypto assets is to be determined under the Rome I Regulation, a distinction must be made according to the role of the crypto assets in the respective contractual relationship and whether crypto assets are the subject of performance of only one or both contracting parties.

A contract by which crypto assets are acquired in exchange for a fiat currency could be classified as a sale of goods, with crypto assets characterised as a "good" within the meaning of Article 7(1)(b) of the Brussels I*bis* Regulation and Article 4(1)(a) of the Rome I Regulation.[80] According to the case law of the CJEU and legal scholars, a "good" in this sense can only be a tangible, movable thing.[81] The concept of a tangible, movable thing is not exclusively used by the Rome I Regulation, but also describes, for example, a legal category in international

79 Guiliano and Lagarde (n 75), 11 with regard to the purchase and sale of those negotiable instruments.

80 According to Recital 17 of the Rome I Regulation, the term "sale of goods" is to be interpreted in parallel with the Brussels Convention, a predecessor of the Brussels I*bis* Regulation, and also in parallel with the Brussels I*bis* Regulation; McParland (n 62), para. 10.99.

81 CJEU Case C-381/08 *Car Trim GmbH* v *KeySafety Systems Srl* [2010] EU:C:2010:90, para. 35; Franco Ferrari and Jan Bischoff, "Article 4," in Franco Ferrari (ed), *Concise Commentary on the Rome I Regulation* (2nd edn, Cambridge University Press 2020), para. 17.

succession law (Article 30 Succession Regulation) and in international property law.

Although the scope of application of the various conflict-of-laws rules relating to goods and the respective rule-making bodies are very different, all these provisions have in common that the good must have the quality of corporeality regarding the prerequisites for the existence of a movable thing.[82] Therefore, the existence of a good within the meaning of the various conflict-of-laws rules always requires the movable thing to be delimited in space. This applies even if the substantive concept of "goods" within the respective legal order is in principle broader and encompasses incorporeal objects.[83]

However, crypto assets lack the corporeality required in this respect, as they are neither directly perceptible to the senses nor controllable by humans. Furthermore, the determination of the applicable law through these conflict-of-laws rules is sometimes complicated by the fact that the connecting factor of these rules is the place where the object is located. For crypto assets, this place cannot be determined, or can only be established with difficulty and in a purely normative manner.

Thus, in principle, crypto assets are not to be classified as movable things for the purposes of conflict of laws. Insofar as crypto assets are the subject of contractual obligations falling within the scope of the application of the Rome I Regulation, and as far as crypto assets represent the performance characteristic of the contract, the law applicable to these contracts is therefore determined according to Articles 4(2)-(4) of the Rome I Regulation. Hence, if the subject of the legal analysis is a contract in which the crypto asset represents the characteristic performance of the contract according to the type of contract and the distribution of rights and obligations,[84] the habitual residence of the person who undertakes to transfer the crypto asset is decisive for determining the applicable law (Article 4(2) of the Rome I Regulation). A contract, the performance of which is characterised by the transfer of crypto assets, is regularly given if the crypto asset is transferred in exchange for fiat currency, but also if a non-native crypto asset is exchanged for a native crypto asset. According to the expectations of the contracting parties, the native crypto asset regularly has a payment function in relation to the non-native crypto asset. If, in contrast, native crypto assets are exchanged for native crypto assets or non-native

82 Magnus (n 42), para. 60; Ferrari and Bischoff (n 80), para 17.

83 This applies, for example, to Austrian law, which explicitly requires a "corporeal thing" for international property law. See § 31(1) of the Austrian "Federal Act of 15 June 1978 on Private International Law (PIL Act)," (hereafter "Austrian IPRG").

84 Magnus (n 42), para. 176.

crypto assets are exchanged for each other, a characteristic performance of the contract cannot be established. In these cases, the applicable law is to be determined based on the closest connection with recourse to Article 4(4) of the Rome I Regulation.

Furthermore, crypto assets can also be used as remuneration for goods and services that are not crypto assets or represented by them. In these cases, it is questionable whether there is a contract of sale of goods or a contract for the provision of services within the meaning of Articles 4(1)(a)-(b) of the Rome I Regulation. Such a classification could be denied on the basis that these two types of contracts require a certain type of remuneration.

The transfer of crypto assets in exchange for a service does not preclude a classification as a service contract within the meaning of Article 4(1)(b) of the Rome I Regulation. It is disputed whether a contract for the provision of services within this meaning exists where the service is provided without any remuneration.[85] The very existence of this discussion presupposes a rather broad understanding of the concept of service contract. A contract for the provision of services within the meaning of Article 4(1)(b) of the Rome I Regulation does not necessarily require an agreement on the provision of a remuneration in money. Thus, if one party undertakes to provide a service and the parties agree on a remuneration in the form of a crypto asset, a service contract within the meaning of Article 4(1)(b) of the Rome I Regulation may exist.

Something else applies, however, regarding contracts for the sale of goods within the meaning of Article 4(1)(a) of the Rome I Regulation. This provision is to be interpreted in parallel to Article 1(1) of the CISG and Article 2(5) of the Consumer Rights Directive (2011/83/EU).[86] A contract of sale in the sense of Article 4(1)(a) of the Rome I Regulation thus presupposes the exchange of goods for money.[87] Accordingly, contracts in which neither contracting party undertakes to pay money should not be regarded as a contract of sale within the meaning of either Article 4(1)(a) of the Rome I Regulation nor Article 1(1) of the CISG. Hence, these contracts would not be covered by Article 4(1)(a) of the Rome I Regulation,[88] but would instead be subject to Article 4(4) of the Rome I Regulation.[89] But even if one were to follow this approach, it would remain

85 See Ferrari and Bischoff (n 80), para. 26 with further references.

86 McParland (n 62), para. 10.121.

87 McParland (n 62), para. 10.120; see for the corresponding interpretation under the CISG also Loukas Mistelis, "Article 1 CISG," in Stefan Kröll, Loukas Mistelis, and Pilar Perales Viscasillas (eds), *UN Convention on Contracts for the International Sale of Goods* (2nd edn, C.H. Beck, Nomos and Hart 2018), paras. 26, 30.

88 Magnus (n 42), para. 291.

89 Torremans et al. (n 45), 727 Fn. 446; McParland (n 62), para. 10.129.

questionable what is to be meant by money within the meaning of Article 4(1)(a) of the Rome I Regulation. As far as is apparent, there is no requirement that the performance owed must be state-issued currencies with legal tender quality. Thus, crypto assets could also potentially be money in this sense.

For determining which objects of performance are to be understood as money in this sense, the structure of Article 4 of the Rome I Regulation must be examined more closely. The connecting factors contained in Articles 4(1)(a) and (b) of the Rome I Regulation are examples of the principle of linking the contractual relationship to the performance characteristic of the contract as laid out in Article 4(2) of the Rome I Regulation.[90] The establishment of the link to the performance characteristic of the contract is based on the reasoning that the party performing the obligation characteristic of the contract has a greater interest in the application of the law with which it is familiar. The obligations characteristically resulting from the contract are more complex, require a more comprehensive regulation and constitute the core of the exchange of performances.[91] Also, the party rendering the performance characteristic of the contract regularly acts on a professional basis and in a multitude of cases. This is why it is more intensively affected by the applicable law than the other party to the contract.[92] The performance giving the contract its specific character distinguishes it from other types of contracts and enables it to be classified as characteristic of the contract.[93] The recourse to the performance specific to the contract links the contract to its economic and social embeddedness.[94] With regard to the payment of money, this is regularly not the performance characterising the contract, since money as a means of exchange is nothing special and the payment does not presuppose any special knowledge, skills, or specialisation.[95]

Considering these fundamental observations on the relationship between Article 4(1)(a) of the Rome I Regulation and Article 4(2) of the Rome I Regulation, crypto assets can also serve the function of a means of payment and thus be considered as "money" in contracts of the sale of goods. Accordingly, if the parties to a contract agree to exchange a movable thing for a fungible crypto asset, this contract is a contract for the sale of goods within the meaning of

90 Magnus (n 42), para. 38.
91 Magnus (n 42), para. 169.
92 Bernd von Hoffmann, "General Report on Contractual Obligations," in Ole Lando, Bernd von Hoffmann, and Kurt Siehr (eds), *European Private International Law of Obligations* (J.C.B. Mohr 1975), 8.
93 Magnus (n 42), para. 175.
94 Guiliano and Lagarde (n 75), 1, Art. 4 para. 3.
95 Ferrari and Bischoff (n 80), para. 68.

Article 4(1)(a) of the Rome I Regulation. A fungible crypto asset has a remuneration function. The contract including such a fungible crypto asset is thus not about the performance of a certain crypto asset – the agreement of such a performance would not even be possible due to the technical design of fungible crypto assets – but about the transfer of crypto assets as remuneration for the moveable thing. According to the intention of the parties and based on an economic approach, the crypto asset is a substitute for the otherwise owed monetary payment. This is shown by the fact that the obligation can sometimes be fulfilled either by the transfer of crypto assets or by the transfer of an amount in fiat currency – for example in contracts with Whole Foods or Starbucks.[96] Moreover, bad performance of the crypto assets, which would lead to the need to apply complex regulations, is excluded due to the purely amount-based liability. Also, in other respects, there is no need for extensive regulations with respect to the obligation to render performance based on crypto assets. Fungible crypto assets, as counter-performance, thus have the function of remuneration in contracts for the sale of goods.

The importance of this finding for the determination of the law applicable to contractual obligations must not be underestimated: In this respect, it should first be noted that there is no need to differentiate between the various functions that crypto assets may have. Also, regardless of whether it is a crypto asset with merely intrinsic value (native crypto asset) or one with extrinsic value (non-native crypto asset), the debtor in a contract of sale of goods only undertakes to transfer a certain amount of the crypto asset. The right, represented by and possibly underlying the crypto asset – as the two parties to the contract know – is not influenced by the debtor, but only by the issuer of the respective crypto asset. Therefore, non-native crypto assets can in principle also be subject to a sale of goods within the meaning of Article 4(1)(a) of the Rome I Regulation, insofar as the parties do not intend the asset to be located outside the blockchain, but instead intend this asset to merely stabilise the value of the crypto asset. If, however, the parties' aim in concluding the contract is precisely the transfer of the asset outside the blockchain on which the crypto asset is based, the crypto asset in question does not merely serve as a means of payment. In these cases, there is no sale of good within the meaning of Article 4(1)(a) of the Rome I Regulation and the law applicable to the contract is determined by Article 4(4) of the Rome I Regulation. Furthermore, the

96 Michael del Castillo, "Customers Can Spend Bitcoin At Starbucks, Nordstrom And Whole Foods, Whether They Like It Or Not" (*Forbes*, 13 May 2019) <https://www.forbes.com/sites/michaeldelcastillo/2019/05/13/starbucks-nordstrom-and-whole-foods-now-accept-bitcoin-just-dont-ask-them/> accessed 30 June 2023.

categorisation of crypto assets as remuneration is not only limited to contracts of sale of goods, but can in principle be applied to all types of contracts listed in Article 4(1) of the Rome I Regulation where a performance characteristic of the contract exists.[97]

Particular care, nonetheless, must be taken when examining the parties' intentions if the crypto assets are not fungible. In these cases, at least theoretically, the denomination in crypto assets may, according to the parties' intentions, not only be a quantitative obligation, but an obligation relating to specific crypto assets. It is not possible to give a generally valid answer as to whether in these cases the crypto assets are still to be seen as remuneration within the meaning of the contracts listed in Article 4(1) of the Rome I Regulation. In this respect, a precise examination of the parties' expectations and the significance of commerce is needed with respect to the non-fungible crypto assets.

Moreover, crypto assets as the subject of a contract may influence the determination of the applicable law if the contracting parties are a consumer and a professional. In this case, the applicable law is determined in deviation from Articles 3 and 4 of the Rome I Regulation, according to Article 6 of the Rome I Regulation. In principle, this applies irrespective of the subject matter of the contract. However, according to Article 6(4)(d) of the Rome I Regulation, Articles 6(1) and (2) of the Rome I Regulation do not apply to rights and obligations in connection with financial instruments or in connection with the issuing or public offering of financial instruments. In this respect, it is therefore questionable whether crypto assets might qualify as financial instruments within the meaning of this definition.

As follows from Recital 30 of the Rome I Regulation, in conjunction with Article 94(2) of the MiFID II, the term "financial instrument" is defined in accordance with Article 4(1)(15) of the MiFID II. Article 4(1)(15) of the MiFID II, in conjunction with Annex I Section C of the MiFID II, contains an exhaustive list of financial instruments. The term financial instrument is thus a generic term that covers diverse types of instruments. Even if one would have categorically excluded the classification of crypto assets as financial instruments so far, for example because crypto assets did not yet exist when MiFID II was created, this exclusion can no longer be upheld. According to the will of the European Commission, the phrase "including instruments issued by means of distributed ledger technology" is to be added to the definition of financial instrument in Article 4(1)(15) of the MiFID II by Article 6(1) of the draft Directive on

97 Namely Art. 4(1)(a), b), e), and (f). See Lord Collins of Mapesbury and Harris (n 45), vol. 1, para. 32-075.

the Extension of the MiFID II.[98] This addition shall have merely a clarifying effect.[99] Thus, crypto assets, at least if the Directive actually enters into force in this form, are potentially financial instruments within the meaning of the MiFID II. The European Commission's reference to the clarifying effect shows that crypto assets – at least according to the will of part of the legislative body – can be classified as financial instruments within the meaning of the MiFID II already nowadays if the further requirements are met. In principle, the categorisation of crypto assets as financial instruments is therefore possible.

Whether crypto assets are in fact to be classified as a type of financial instrument hinges on the function of the respective crypto asset. The classification of native crypto assets as financial instruments within the meaning of the MiFID II was described by ESMA as unlikely.[100] Apart from this, the classification of crypto assets as financial instruments is highly controversial and, according to a prevailing opinion, depends strongly on the individual design of the respective crypto asset.[101] The questions of whether the applicability of Article 6(1) of the Rome I Regulation to a contract between a consumer and a professional concerning a crypto asset is excluded under Article 6(4)(d) of the Rome I Regulation, and whether the applicable law is to be determined according to Article 4 of the Rome I Regulation thus depends significantly on the specific design of the individual crypto asset and the future positions of supervisory authorities as well as legal scholars. In this respect, it can, at best, be said in a generalised manner that native crypto assets in this sense are typically not financial instruments.[102] In contrast, non-native crypto assets may be classified as a type of financial instrument if they serve at least an investment

98 Proposal for a Directive of the European Parliament and of the Council amending Directives 2006/43/EC, 2009/65/EC, 2009/138/EU, 2011/61/EU, EU/2013/36, 2014/65/EU, (EU) 2015/2366 and EU/2016/2341, 2020/0268(COD).

99 *Id.*, 5.

100 European Securities and Markets Authority (n 17), 19 para. 80.

101 See exhaustively on the question of whether crypto assets qualify as financial instruments and especially as securities within the meaning of European capital markets regulation, Hacker and Thomale (n 17), 663–687; Ferrari (n 6), 330–332; Vlad Burilov, "Regulation of Crypto Tokens and Initial Coin Offerings in the EU" (2019) 6 European Journal of Comparative Law and Governance 146, 163–174; Constantin Frank-Fahle, Benjamin Sauter, and Jörg Schmidt, "Regulatory Framework on ICO in the USA, UAE, Germany and Japan" (2019) Zeitschrift für Internationales Wirtschaftsrecht 122, 127–128; European Securities and Markets Authority (n 17), paras. 77–89 and Annex I paras. 43–54.

102 In this respect for "currency token", but apparently only those tokens that do not embody any value outside the blockchain, and can thus be equated with native crypto assets, are meant: Maume and Fromberger (n 17), 577; Dickinson (n 56), para. 5.51; Hacker and Thomale (n 17), 676.

purpose.[103] However, this is only a very rough approximation, which hardly allows any conclusions to be drawn for individual tokens.

3.2.1.3 *The Particular Circumstances of the Acquisition and Transfer of Crypto Assets as a Factor in Determining the Applicable Law*

Finally, the determination of the applicable law for crypto assets may also be influenced by the circumstances of the acquisition and transfer of crypto assets in individual cases. The Rome I Regulation modifies the determination of the applicable law in various provisions for those cases, in which special circumstances accompany the actual conclusion of the contract.

Such a modification can be found first in Article 4(1)(h) of the Rome I Regulation, according to which the determination of the applicable law is subject to special provisions if the contract is concluded via a multilateral system and if the subject matter of the contract is financial instruments. In particular, such contracts could be the purchase and sale of crypto assets. As seen, crypto assets may be classified as financial instruments depending on their individual properties. In contrast, it is questionable whether and when the trading of crypto assets which can be classified as financial instruments takes place via a multilateral system within the meaning of Article 4(1)(h) of the Rome I Regulation. The blockchain itself only documents the individual transfers and thus has no influence on the conclusion of the contract itself. In contrast, the crypto exchange through which crypto assets are regularly traded could be classified as such a multilateral system. Contracts concluded on this exchange would then be subject to a unified law in accordance with Article 4(1)(h) of the Rome I Regulation. However, this presupposes that a crypto exchange can be categorised as a multilateral system. Recital 18 of the Rome I Regulation defines multilateral system in reference to Article 4 of the MiFID I.[104] This Directive has been replaced by the MiFID II, whereby references to the MiFID I are to be understood as references to the MiFID II.[105] According to Article 4(1)(19) of the MiFID II, a multilateral system is "a system or mechanism that brings together multiple third-party buying and selling interests in financial instruments within the system."

---

103 Hacker and Thomale (n 17), 671–680, 686; for investment tokens see Philipp Maume, "Initial Coin Offerings and EU Prospectus Disclosure" (2020) 31 European Business Law Review 185, 192–193.

104 Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments amending Council Directives 85/611/EEC and 93/6/EEC and Directive 2000/12/EC of the European Parliament and of the Council and repealing Council Directive 93/22/EEC [2004] OJ L145/1 (hereafter "MiFID I").

105 Art. 94, subpara. 2 of the MiFID II.

Due to the broad nature of this definition, a crypto exchange might be such a system within the meaning of Article 4(1)(19) of the MiFID II. This definition is not limited by Recital 18 of the Rome I Regulation, which only refers to regulated markets and multilateral trading facilities within the meaning of the MiFID I. This enumeration should not be understood to indicate that only these two types of systems can be multilateral systems within the meaning of Article 4(1)(h) of the Rome I Regulation, and that Article 4(1)(19) of the MiFID II is useless to define the term multilateral system within the meaning of the Rome I Regulation.[106] As follows from the wording of Recital 18 of the Rome I Regulation, the enumeration is merely exemplary ("such as"). At the same time, however, the reference to the MiFID I makes it clear that a definition of the term is sought which runs parallel to this directive. If, according to the will of the European legislator, the MiFID II replaces the MiFID I, and if references to the latter Directive are to be understood as references to the MiFID II (Article 94 of the MiFID II), the definition of the multilateral system in Article 4(1)(19) of the MiFID II is to also form the basis of the Rome I Regulation. The mere indirect reference of Recital 18 of the Rome I Regulation to the corresponding legal definition of the multilateral system in the MiFID II can be easily explained by the lack of a legal definition of this term in the MiFID I.[107]

However, a contract for a financial instrument concluded within a multilateral system is only covered by Article 4(1)(h) of the Rome I Regulation if trading through that system takes place under non-discretionary rules and the trading is governed by a single law. Whether these conditions are met for the respective crypto exchange cannot be assessed in an abstract and blanket manner. In this respect, an examination of the individual case is always required. To this extent, it is also always necessary to examine the seat, the targeted customer base, and the general terms and conditions of the respective crypto exchange in detail. However, it is not ruled out from the beginning and is mostly within the power of the crypto exchange operator to conduct its trading based on a single law and by means of non-discretionary rules.

If the crypto asset in the individual case is to be classified as a financial instrument (see *supra* 3.2.1.2) and the respective crypto exchange is a multilateral system within the meaning of the MiFID II, the law applicable to contracts concluded via crypto exchanges which have crypto assets as their object might be determined by the law to which the crypto exchange is subject, if the further requirements of Article 4(1)(h) of the Rome I Regulation are also met. These

106 See also Matthias Lehmann, "Financial Instruments," in Franco Ferrari and Stefan Leible (eds), *Rome I Regulation* (Sellier 2009), 88.

107 Regarding this result, see also Ferrari and Bischoff (n 80), para. 56.

are, in addition to the non-discretionary rules and the uniform law, in particular the bringing together of multiple third-parties buying and selling interests.

The considerations set out above become also particularly relevant if the obligation for which the applicable law is to be determined involves a consumer and a professional within the meaning of Article 6(1) of the Rome I Regulation. According to Article 6(4)(e) of the Rome I Regulation, the law applicable to a contract between a consumer and a professional is not determined by Article 6 of the Rome I Regulation if the contract is concluded within a system to which Article 4(1)(h) of the Rome I Regulation applies. If a contractual obligation is subject to Article 4(1)(h) of the Rome I Regulation, the law applicable to it is thus determined independently of the consumer status of a contracting party.[108] For contracts on crypto assets concluded on crypto exchanges, this implies the determination of the law applicable to a contract between a consumer and a professional according to Article 4(1)(h) of the Rome I Regulation, in derogation from Article 6(1) of the Rome I Regulation, if the requirements set out in Article 4(1)(h) of the Rome I Regulation are met.

3.2.1.4 *Contracts on the Transfer of Crypto Assets*

Part of the question of how crypto assets are to be classified from a conflict-of-laws perspective is the question of what law governs the transfer of crypto assets. However, the question of which law applies to the transfer of crypto assets depends crucially on how crypto assets are qualified under the conflict of laws. For instance, crypto assets could be classified as claims leading to the transfer of crypto assets taking place according to the rules for claims by way of assignment. By contrast, the transfer could also be governed by the rules for property.[109] Thus, the law applicable to the transfer of crypto assets depends to a large extent on whether crypto assets can be classified as a thing or a claim under conflict of laws. Therefore, it must first be examined whether crypto assets classify as a claim within the meaning of the conflict-of-laws rules on assignment.

Conflict-of-laws rules on assignment are to be found in Article 14 of the Rome I Regulation. Article 14(1) of the Rome I Regulation contains rules on the relationship between the assignor and the assignee. Article 14(2) of the Rome I Regulation regulates the relationship between the assignee and the debtor. Article 14(1) of the Rome I Regulation and Article 14(2) of the Rome I Regulation both require for their applicability the transferred object to be categorised as a claim. A claim within this meaning is the right to claim a debt of whatever kind,

108 Recital 28, sentence 3 of the Rome I Regulation.

109 See on this below 3.2.4.1.

irrespective of whether it is monetary or non-monetary or whether it results from a contractual or non-contractual obligation.[110] Following this definition, crypto assets themselves – regardless of whether they are native or non-native crypto assets and whether these crypto assets are fungible or non-fungible – cannot be categorised as a claim.[111] For native crypto assets, this already follows from the fact that the holding of such an asset does not establish any right to claim a debt. This applies regardless of the type of blockchain on which the crypto asset is transferred. For those who only hold crypto assets without participating in the operation of the blockchain, the technical design of the blockchain is usually of secondary importance. For the holders of crypto assets, the blockchain is only a means to an end to ensure a technically unambiguous attribution of the actual possibility of transferring crypto assets. In addition, in the case of a public permissionless blockchain, there is regularly no intention on the part of the participants to be legally bound.[112] While non-native crypto assets represent a corresponding right, they cannot be equated with the right itself. The crypto asset and the claim can each exist and are, in principle, each subject to an independent regulation. Whether the legal fate of a crypto asset and a claim can be linked is a question of the respective substantive law and not logical or legally compelling. Thus, non-native, as well as native, crypto assets are subject to an independent legal assessment. Accordingly, due to the lack of a right directly resulting from the holding of the non-native crypto asset as such, a classification of the non-native crypto asset as a claim is excluded.

Thus, crypto assets are not to be characterised as a claim within the meaning of Article 14 of the Rome I Regulation. The law applicable to the transfer of crypto assets is therefore not determined by Article 14 of the Rome I Regulation. However, as we have already seen (see 3.2.1.2), a characterisation of crypto assets as a thing is also not possible, irrespective of their specific design. Thus, a determination of the law applicable to the transfer of crypto assets according to the rules of international property law is likewise excluded.

3.2.2 The Characterisation of Crypto Assets within Non-Contractual Relations

Claims under the law of obligations between persons can be established not only by way of a contract but also in other ways. This is especially the case with

110 See Dickinson (n 56), para. 5.101, referring to Article 2(d) of the European Commission's Proposal for a Regulation of the European Parliament and of the Council on the law applicable to the third-party effects of assignments of claims [2018] COM/2018/096 final.

111 See Dickinson (n 56), paras. 5.101, 5.106.

112 See on this above 3.2.1.1.

crypto assets, for example, if the crypto assets are not transferred to the key pair to which the transferor intended them to be transferred due to a typing error or other mistake, or if a person gains unauthorised access to the crypto assets and transfers them to a key pair that only he controls. If the existence of such claims is questionable and there is no contract between the creditor and the debtor, the law applicable to the potential obligation is determined by the Rome II Regulation. Regarding international jurisdiction for claims arising from non-contractual obligations, Article 7 No. 2 of the Brussels I*bis* Regulation may apply. Since the applicability of Article 7 No. 2 of the Brussels I*bis* Regulation depends exclusively on the type of obligation underlying the respective claim, irrespective of the legal object of the obligation, there are no special considerations for crypto assets in this respect.

The applicability of the Rome II Regulation to non-contractual obligations involving crypto assets is not excluded according to Article 1(2)(c) of the Rome II Regulation or Article 1(2)(d) of the Rome II Regulation. For Article 1(2)(c) of the Rome II Regulation, what has already been said about the identically worded Article 1(2)(d) of the Rome I Regulation applies.[113] Article 1(2)(d) of the Rome II Regulation does also not exclude the application of the Rome II Regulation, since a blockchain network cannot be classified as a company within the meaning of European conflict of laws.[114]

Crypto assets can be the subject of a non-contractual obligation within the meaning of the Rome II Regulation. As with the Rome I Regulation, the applicability of the Rome II Regulation does not depend on the object to which the claim asserted in detail relates.[115] For the determination of the applicable law, it makes no difference in principle whether crypto assets or other assets are transferred by mistake or whether they are removed from the access of the original holder. The Rome II Regulation defines in Article 2 the concept of damage in a deliberately broad way and understands it to include all consequences of a tortious act, unjust enrichment, *negotiorum gestio*, or *culpa in contrahendo*. Therefore, it also covers cases in which someone has gained something by interfering with the claimant's legal position without a corresponding damage having occurred on the claimant's side.[116]

For the determination of the law applicable to an obligation, it should be noted that the terms – at least for the delineation of the scope of application

113 See above 3.2.1.2.

114 See already on this above 3.2.1.1.

115 See on this with regard to the Rome I Regulation, infra 3.2.1.2.

116 Axel Halfmeier, "Art 2 Rome II Regulation," in Gralf-Peter Calliess and Moritz Renner (eds), *Rome Regulations* (3rd edn, Wolters Kluwer 2020), para 7.

of the Rome I Regulation and the Rome II Regulation – of contractual and non-contractual obligations are complementary to each other. A claim under the law of obligations that is not capable of being characterised as contractual is thus a non-contractual claim within the meaning of the Rome II Regulation.[117] Claims arising from a non-contractual obligation resulting from a transfer of crypto assets must therefore be assessed according to the Rome II Regulation if the further requirements of Article 1 of the Rome II Regulation are met.

As seen, the Rome II Regulation in principle does not determine the applicable law depending on the object of damage, but rather depending on the non-contractual obligation giving rise to the claim.[118] Thus, for the determination of the applicable law under the Rome II Regulation, it is in principle not relevant what the subject matter of the asserted claim is or how crypto assets are protected in detail by the substantive law of non-contractual obligations. However, the Rome II Regulation provides some exceptional special connecting rules if the damage was caused by a specific means (see 3.2.2.1) or occurred to a specific asset (see 3.2.2.2). The extent to which crypto assets can be classified as such a mean or as such an asset will be examined in the following.

3.2.2.1 *Special Connecting Rules of the Rome II Regulation in the Case of Damage Caused by a Specific Means*

Article 5 of the Rome II Regulation provides special rules for the determination of the applicable law if damages are caused by a product. These conflict-of-laws rules can become relevant, for example, if a loss of the crypto asset or a decrease in the value of the crypto asset occurs due to an error in the programming of the smart contract underlying the crypto asset or of the blockchain. However, it is questionable whether crypto assets can be a product within the meaning of this provision and whether Article 5 of the Rome II Regulation also covers damages occurring to the product itself and damages that are merely an economic loss.

Regarding the question whether crypto assets can be characterised as a product within the meaning of Article 5 of the Rome II Regulation, the Rome II Regulation itself contains no indication of what is to be understood by a "product". Accordingly, it is disputed how the concept of product within the meaning of Article 5 of the Rome II Regulation is to be defined. Some refer

117 Lüttringhaus (n 78), paras. 4, 7, 10; McParland (n 62), para. 6.07.

118 For claims in tort the applicable law is determined by Article 4 of the Rome II Regulation; for claims in *culpa in contrahendo* by Article 12 of the Rome II Regulation; and for claims *in negotiorum gestio* by Article 11 of the Rome II Regulation.

to Article 2 of the Product Liability Directive[119] and the need for a uniform interpretation of the legal acts of the European Union.[120] Others emphasise the explicit reference to the Product Liability Directive being originally made during the legislative process, but not discussed later.[121] Also, the restriction to products within the meaning of the Directive would narrow the scope of application of Article 5 of the Rome II Regulation too much and would not take sufficient account of the needs of conflict of laws.[122] Therefore, some see a product as any good with monetary value which can be the subject of commercial transactions.[123] For crypto assets, however, these different definitions are only relevant if Article 2 of the Product Liability Directive requires the corporeal nature of a thing as an inherent characteristic of the definition. Crypto assets and their underlying smart contracts or blockchains may be based exclusively on incorporeal program code.

A definition of product within the meaning of Article 5 of the Rome II Regulation presupposing corporeality would thus lead to the applicable law being determined not according to Article 5 of the Rome II Regulation, but Article 4 of the Rome II Regulation.[124] However, it is disputed whether the concept of product in Article 2 of the Product Liability Directive presupposes the corporeality of the product.[125] At any rate, those who support the reference to Article 2 of the Product Liability Directive for the interpretation of Article 5 of the Rome II Regulation argue against such a narrow understanding of the

119 Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products [1985] OJ L210/29.

120 Christoph Schmid and Tobias Pinkel, "Art 5 Rome II Regulation," in Gralf-Peter Calliess and Moritz Renner (eds), *Rome Regulations* (3rd edn, Wolters Kluwer 2020), para. 11; see also Martin Illmer, "Art. 5 Rome II," in Peter Huber (ed), *Rome II Regulation* (Sellier 2011), para. 12; Guillermo Palao Moreno, "Product liability: jurisdiction and applicable law in cross-border cases in the European Union" (2010) 11 ERA Forum 45, 55.

121 Giorgio Risso, "Product liability and protection of EU consumers: is it time for a serious reassessment?" (2019) 15 Journal of Private International Law 210, 217.

122 See also exhaustively on this point Richard Plender and Michael Wilderspin, *The European Private International Law of Obligations* (5th edn, Sweet & Maxwell 2020), paras. 19-015–19-033; similar Piotr Machnikowski, "Art 5 Rome II," in Ulrich Magnus and Peter Mankowski (eds), *European Commentaries on Private International Law Volume III Rome II Regulation* (Otto Schmidt 2019), para. 47.

123 Plender and Wilderspin (n 122), para. 19-026.

124 *Id*., para. 19-018.

125 Discussing the question of the requirement of corporeality for intellectual products, see Duncan Fairgrieve and Richard S Goldberg, *Product Liability* (3rd edn, Oxford University Press 2020), paras. 9.77–9.84, 9.104.

concept of product.[126] Thus, the vast majority of the literature assumes, at least for the purposes of Article 5 of the Rome II Regulation, incorporeal objects being products within the meaning of Article 5 of the Rome II Regulation. Crypto assets can therefore be classified as products at least within the meaning of Article 5 of the Rome II Regulation if the further requirements are met.

Also, there is widespread agreement that damage within the meaning of Article 5 of the Rome II Regulation is, in deviation from the Product Liability Directive, also damage to the product itself and economic damage caused by the product.[127] If, as a result of an error in the programming of the crypto asset, there is a loss of the crypto asset or a loss of value, the law applicable to claims against the issuer of the crypto asset might thus be determined by Article 5 of the Rome II Regulation.

3.2.2.2 *Crypto Assets as Assets Particularly Protected by the Rome II Regulation*

In deviation from the general conflict-of-laws rules, the applicable law to non-contractual obligations regarding intellectual property rights, according to Articles 8 and 13 of the Rome II Regulation, is determined by the law of the country for which the protection of intellectual property is claimed. If crypto assets such as Bitcoin, Ether or BNB were to be characterised as intellectual property rights in this sense, the applicable law to non-contractual obligations would have to be determined depending on the respective country for which claims are asserted.

The concept of intellectual property is to be interpreted autonomously and in accordance with Recital 26 of the Rome II Regulation.[128] Assuming an autonomous characterisation,[129] the term is to be interpreted broadly and flexibly.[130] It covers all different types of national, regional, or international exclusive rights that may be designated as intellectual property.[131] The only prerequisite

126 Schmid and Pinkel (n 120), para. 10.

127 Lord Collins of Mapesbury and Harris (n 45), vol. 2, para. 35–042; Machnikowski (n 122), para. 29; Plender and Wilderspin (n 122), paras. 19-037, 19-042; Schmid and Pinkel (n 120), para. 20.

128 Plender and Wilderspin (n 122), paras. 22-010–22-011.

129 This is disputed; *e.g.*, in German legal scholarship, see Karl-Heinz Fezer and Stefan Koos, "Internationales Immaterialgüterprivatrecht," in Ulrich Magnus (ed), *J. von Staudingers Kommentar zum Bürgerlichen Gesetzbuch: Internationales Wirtschaftsrecht* (Sellier/de Gruyter 2019), para. 914 *et seq*.

130 Martin Illmer, "Art. 8 Rome II," in Peter Huber (ed), *Rome II Regulation* (Sellier 2011), para. 5.

131 Axel Metzger, "Art 8 Rome II," in Ulrich Magnus and Peter Mankowski (eds), *European Commentaries on Private International Law Volume III Rome II Regulation* (Otto Schmidt 2019), para. 9.

is that a right is granted and the right holder is exclusively entitled to it.[132] For the characterisation as an intellectual property right within the meaning of Articles 8 and 13 of the Rome II Regulation, the structuring of the respective intellectual property within the substantive law of the state for which these rights are asserted is decisive.[133]

For crypto assets, this means a significant dependence on the characterisation of a right to a crypto asset as an intellectual property right and the determination of the law applicable to it on how the rights to crypto assets are structured in detail under the law of the respective country for which the right is claimed, and which legal basis is used to substantiate the respective claim.[134]

3.2.3 Special Conflict-of-Laws Rules for Special Legal Objects: Crypto Assets as Personal Data?

Under certain circumstances, substantive law provides special rules for certain legal interests. As a rule, these are cross-sectional matters which, due to the special characteristics of the respective object of regulation, elude the common classification of claims. If the special characteristics of these legal interests also require a different determination of the applicable law and are thus accompanied by special conflict-of-laws rules, the question arises from a conflict-of-laws perspective as to whether subsumption under the legal category of this special conflict-of-laws rule is possible. An example of such a special treatment at the level of substantive law and conflict of laws is the GDPR.[135] It attaches special duties of conduct and, where applicable, obligations to pay damages (Article 82 of the GDPR) to the handling of personal data. It also provides its own conflict-of-laws rule in Article 3 of the GDPR and its own rule on international jurisdiction in Article 79(2) of the GDPR.

---

132 James J. Fawcett and Paul Torremans, *Intellectual Property and Private International Law* (2nd edn, Oxford University Press 2011), para. 15.20.

133 Mary-Rose McGuire, "Art. 8 Rom II-VO," in Christine Budzikiewicz, Marc-Philippe Weller, and Wolfgang Wurmnest (eds), *beck-online.GROSSKOMMENTAR Rom II-VO* (C.H. Beck 2021), para. 108; similar, Andrew Dickinson, *The Rome II Regulation* (Oxford University Press 2010), para. 8.13.

134 See in this respect Plender and Wilderspin (n 122), para. 22-021, who describes a situation where a claim can be based on both intellectual property infringement and unfair competition.

135 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

This raises the question of whether crypto assets can be classified as personal data within the meaning of Article 3 of the GDPR.[136] According to Article 4(1) of the GDPR, personal data are information relating to an identified or identifiable natural person. A natural person is identifiable, inter alia, if he or she can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, or an online identifier (Article 4(1) of the GDPR). Indirect identification is given if the data merely allow recognition. The decisive factor is whether the data controller or another person can identify the data subject by the means reasonably used.[137] Based on this assessment, the public key, insofar as it can be assigned to a natural person and independently of the type of crypto asset assigned to it, is to be classified as personal data within the meaning of Article 4 of the GDPR.[138] The public key used in a transaction is usually communicated outside the blockchain to the contracting party and therefore allows at least the latter to link the public key to a natural person. The same applies to any type of crypto asset which is nothing else than the results of the transactions stored on the blockchain or a balance variable in a smart contract and which are in both cases unambiguously assigned to a public key.[139] If the corresponding key pair is used by a natural person, the crypto assets are therefore also personal data within the meaning of Article 4 of the GDPR. The processing of a public key and a crypto asset is thus subject to the obligations established by the GDPR (in particular Articles 12–23 of the GDPR) if the other requirements of the GDPR are met. In

136 See on this question also Matthias Berberich and Malgorzata Steiner, "Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers?" (2016) 2 EDPL 422, 423–424.

137 Recital 26 of the GDPR.

138 European Parliamentary Research Service, "Blockchain and the General Data Protection Regulation" (*European Parliamentary Research Service*, July 2019), 26–28 <https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf> accessed 30 June 2023; Michèle Finck, "Blockchains and Data Protection in the European Union" (2017) Max Planck Institute for Innovation & Competition Research Paper No. 18-01, 13 *et seq*. <https://dx.doi.org/10.2139/ssrn.3080322> accessed 30 June 2023.

139 Finck (n 138), 10 *et seq*.; different than Jean Bacon et al., "Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers" (2018) 25 Richmond Journal of Law and Technology 1, 62; see also unclear European Parliamentary Research Service (n 138), 28 *et seq*.; see also Natalie Eichler et al., "Blockchain, data protection, and the GDPR," 5 <https://www.crowdfundinsider.com/wp-content/uploads/2018/06/GDPR_Position_Paper_v1.0.pdf> accessed 30 June 2023.

these cases, the natural person is equally entitled to the rights granted by the GDPR (in particular Articles 24–50 of the GDPR).

3.2.4 The Characterisation of the Transfer of Crypto Assets

So far, the focus has been on the question of which categories of the law of obligations of PIL, as developed by the Brussels I*bis* Regulation, the Rome I Regulation, and the Rome II Regulation of the European Union can be assigned to crypto assets. However, it has not yet been examined to what extent conclusions can be made about how crypto assets are to be classified outside of the harmonised conflict of laws. In view of the multitude of existing national rules of conflict of laws and the different connecting factors potentially used to determine the applicable law, the following explanations must remain fragmentary. They refer, firstly, to those national conflict-of-laws rules having already been harmonised to a large extent, even if there is a lack of a coordinating authority in this respect. Secondly, the national conflict-of-laws rules will be examined in those areas that have a particularly high practical relevance.

3.2.4.1 *The Application of International Property Law to Crypto Assets*

Among the regulations of the first category is international property law. International property law – with a few exceptions[140] – has not been the focus of efforts to unify it at the substantive or conflict-of-laws level. The underlying principles and categories of international property law are largely the same: for movable property as well as for real property, the applicable law is the law of the state in which the property is located (*lex rei sitae*).[141]

However, it is questionable whether the relevant national international property law can apply to crypto assets. In principle, the national rules of international property law link their applicability to the existence of a corporeal

140 Cape Town Convention 2307 U.N.T.S. 285; Convention du 15 avril 1958 sur la loi applicable au transfert de la propriété en cas de vente à caractère international d'objets mobiliers corporels; Geneva Convention on the International Recognition of Rights in Aircraft U.N.T.S. 4492.

141 Louis d'Avout, "Property and proprietary rights," *Encyclopedia of Private International Law* (Edward Elgar 2017), 1429–1430; Gian Carlo Venturini, "Property," *International Encyclopedia of Comparative Law Volume III Private International Law* (Mouton and J.C.B. Mohr 1976), 3, 7.

object[142] and thus distinguish between corporeal and incorporeal objects for the determination of the applicable law.[143]

Accordingly, the subject of regulation of the *lex rei sitae* principle is generally only a corporeal object. The restriction of international property law to corporeal objects applies even if national law assumes a broad concept of property for substantive law and correspondingly also provides the possibility of categorising incorporeal objects as property.[144] For incorporeal objects, in contrast, it is unclear, at least for each respective national conflict of laws, whether their characterisation is based on the principles of property law or the principles that apply to claims.[145] In this context, the characteristic of incorporeality is determined in an internationally uniform manner, irrespective of the formulation of the national conflict of laws. According to this definition, incorporeal objects are those that have no geographical anchorage. They are located where someone who is the owner of the object is present, or where the objects representing the incorporeal object are located.[146] However, irrespective of whether incorporeal objects can be the subject of international property law, the connecting factor of the location of the object is unsuitable for determining the applicable law regarding such objects. For intangible objects, the connecting factor of the

142 See in this regard *e.g.*, Art. 43 of the German Introductory Act to the Civil Code (hereafter "EGBGB") ("Sache," which is understood to be a tangible object; see Karsten Thorn, "Art 43 EGBGB," in *Palandt* (80th edn, C.H. Beck 2021), para. 1; Christiane Wendehorst, "Art. 43 EGBGB," in Jan von Hein (ed), *Münchener Kommentar zum Bürgerlichen Gesetzbuch Band 13* (8th edn, C.H. Beck 2021), para. 16; Jens Prütting, "Art. 43 EGBGB," in Christine Budzikiewicz, Marc-Philippe Weller, and Wolfgang Wurmnest (eds), *beck-online.GROSSKOMMENTAR EGBGB* (C.H. Beck 2021), para 44–48) and § 31 of the Austrian IPRG ("körperliche Sachen").

143 *E.g.*, Torremans et al. (n 45), 1263, 1280; Dominique Bureau and Horatia Muir Watt, *Droit international privé Tome II Partie spéciale* (4th edn, Presses Universitaires de France 2017), 49, 70; Peter Hay et al., *Conflict of Laws* (6th edn, West Academic Publishing 2018), § 19.27.

144 See *e.g.*, Austrian law, where for substantive law things can be both corporeal and incorporeal objects (§ 292 of the Austrian General Civil Code of 1 June 1811 (hereafter "ABGB")), whereas for conflict of laws the concept of things is also broad but the *lex rei sitae* rule for determining the applicable law is limited to corporeal objects (§ 31 of the Austrian IPRG).

145 Kamen Troller, "Industrial and Intellectual Property," *International Encyclopedia of Comparative Law Volume III Private International Law* (J.C.B. Mohr and Martinus Nijhoff 1994), 8; thus, the question of whether the concept of property under international property law also includes incorporeal objects does not depend on the definition of the concept of property in the respective international property law, *cf.* for the possible different approaches Wendehorst (n 142), paras. 11–16 and § 31(2) of the Austrian IPRG.

146 Dário Moura Vincente, "Intellectual property, applicable law," *Encyclopedia of Private International Law* (Edward Elgar 2017), 962; Kamen Troller (n 145), 5.

location of the object can only be determined with difficulty and with recourse to alternative connecting factors.[147] Consequently, for incorporeal objects, the rules of international property law and thus the connecting factors on which it is based are considered unsuitable and inapplicable.[148]

Crypto assets themselves lack a geographical anchorage. They merely constitute the allocation of a de facto transfer possibility of a unit of account or a specific crypto asset – depending on whether the crypto asset is fungible – following the rules of a blockchain protocol. The blockchain itself and any assets linked to the crypto asset in the real world cannot be equated with an asset. They serve at best as an auxiliary criterion for determining the law applicable to the crypto asset. Thus, crypto assets – irrespective of their categorisation and design in the individual case – are incorporeal objects that escape international property law as it applies to corporeal objects.

If rights in crypto assets are thus not subject to the *lex rei sitae* principle, this does not mean, however, that the conflict of laws does not recognise any absolute rights in them. As already seen, from a conflict-of-laws perspective, they can be the subject of intellectual property rights[149] – depending on the individual structure of the respective substantive law – which can grant a right of exclusion and use comparable to the property right. On an individual basis, a national act on PIL may also contain provisions regarding the property right applicable to incorporeal objects. In the rarest of cases, such a regulation can be made in a purely abstract manner, as the objects potentially qualifying as incorporeal objects are very different.[150] In contrast, regulations specifically tailored to crypto assets will be found in legal systems which – like Liechtenstein law – provide substantive regulations for crypto assets.[151] A special conflict-of-laws rule might also be limited to a certain type of crypto asset. For example, German law only provides a special conflict-of-laws rule for non-native crypto assets where the value represented outside the blockchain is a debenture on the holder.[152]

147 For similarity, see Jonathan Hill and Márie Ní Shúilleabháin, *Clarkson & Hill's Conflict of Laws* (5th edn, Oxford University Press 2016), para. 9.25.

148 Christian von Bar and Peter Mankowski, *Internationales Privatrecht Volume II* (2nd edn, C.H. Beck 2019), § 3 para. 12.

149 See above 3.2.2.2.

150 Bureau and Watt (n 143), vol. 1, para. 24–051.

151 Art. 3(2) of the Law of 3 October 2019 on Tokens and TT Service Providers (Token and TT Service Provider Act; TVTG) <https://www.regierung.li/files/medienarchiv/950-6-01-09-2021-en.pdf> accessed 30 June 2023.

152 §§ 32, 1 of the Gesetz über elektronische Wertpapiere vom 3. Juni 2021 (BGBL. 2021 I S. 1423) (German Act on the Introduction of Electronic Securities).

Even apart from international property law for tangible property, conflict of laws can provide rules offering a property-like protection of crypto assets. However, problems may arise regarding the characterisation of crypto assets insofar as the corresponding legal category is not explicitly regulated in the conflict-of-laws rules of the *lex fori*. This may lead to situations in which the conflict-of-laws rules of a given jurisdiction would declare themselves applicable, but the *lex fori* does not provide any conflict-of-laws rules in this respect. This may be due to the absence of a corresponding right in crypto assets at the level of substantive law. In these cases, an application of the law containing corresponding rules on the level of conflict of laws or substantive law would be excluded because of a lack of conflict-of-laws rules of the *lex fori*. These cases should not be confused with the phenomenon, which frequently occurs in the context of characterisation, of the conflict rules referring to a different meaning of the terms used[153] or of an unknown foreign legal institution being subsumed under their own conflict rules.[154] Property rights or property-like rights are widely known. Rather, the problem lies primarily in the respective legal system having limited the legal institution to certain legal interests and another legal system having opened this or a similar legal institution to this legal interest. Thus, the question arises as to how the conflict of laws of the legal system limited to this extent should react to this opening. In other words, it is not a matter of adapting unknown legal institutions to one's own legal system, but of extending legal institutions of domestic law to subjects of regulation that are not covered by the respective legal institution according to domestic law. It is hence not a question of interpreting[155] and subsuming[156] under the respective conflict-of-laws rule. The interpretation leads – as seen – to the result of crypto assets being, in principle, not covered by the provisions of international property law, insofar as there is no special conflict-of-laws rule for incorporeal objects. However, for the purposes of effective legal protection and to establish the state's monopoly on the use of force, there must be no situations escaping legal regulation. The binding of the persons subject to the monopoly on the use of force presupposes the possibility to enforce their claims acknowledged

153 Ernest G. Lorenzen, "The Theory of Qualifications and the Conflict of Laws" (1920) 20 Columbia Law Review, 247.

154 Bariatti (n 53), 358; Michael Bogdan, *Private International Law as Component of the Law of the Forum General Course on Private International Law* (Brill 2011), 148 *et seq*., 216–218.

155 Bariatti (n 53), 357; Michael Bogdan (n 154), 134; Lord Collins of Mapesbury and Harris (n 45), vol. 1, para. 2-007.

156 On the dispute about the precise categorisation of the classification, see Dirk Looschelders, "Einleitung zum IPR," in Dieter Hendrich (ed), *J. von Staudingers Kommentar zum Bürgerlichen Gesetzbuch: Einleitung zum IPR* (Sellier/de Gruyter 2019), para. 1081.

by the legal order with the help of state institutions.[157] In this respect, at the least an express provision is required which explicitly stipulates that a matter is beyond the control of the state. Even the express non-regulation of a matter provides the intention not to regulate a matter and thus not to recognise an enforceable right. Applied to conflict of laws, this entails that the absence of an explicit conflict-of-laws rule for property or property-like rights in crypto assets must not result in the conflict of laws of the *lex fori* leaving the applicable law indeterminate. The identification of the applicable law is a necessary prerequisite for the legal treatment of a cross-border situation.

In the absence of an explicit provision stating the substantive law applying to property rights or property-like rights, rights in crypto assets remain undetermined and the necessity of a conflict-of-laws rule for such legal issues not regulated by the substantive law of the *lex fori* is manifest. This raises the question as to how the law applicable in this respect is to be determined. There seems to be no general solution for the absence of a corresponding provision in the conflict of laws of the *lex fori*. It is also not the task of this contribution to give a conclusive answer to this question. The following remarks are merely intended to point out a possible approach to a solution. Individual, case-oriented, and pragmatic solutions are required, which consider the respective systematics of the conflict of laws of the *lex fori*. In this respect, it should as well be taken into account that not only corresponding rights to crypto assets will regularly be unknown. Also, the connecting factors provided by the conflict of laws of the *lex fori* does not allow for a determination of the applicable law due to the lack of corporeality of the crypto assets.

Thus, recourse will have to be made to the principle of the closest connection. Such recourse is possible in the form of an analogous application of the escape clauses of the conflict-of-laws rules of international property law,[158] the application of a general conflict-of-laws rule,[159] or the use of the principle of the closest connection as a general legal principle in conflict of laws. This principle is widely recognised[160] – at least in continental European conflict

157 *Cf.* Andreas Anter, "The Modern State and Its Monopoly on Violence," in Edith Hanke, Lawrence Scaff, and Sam Whimster (eds), *The Oxford Handbook of Max Weber* (Oxford University Press 2020), 231; see also Stefan Haack, "Monopoly on the Use of Force," in Ludger Kühnhardt and Tilman Mayer (eds), *Bonn Handbook of Globality* (Springer 2019), vol. 1, 1107 (especially on the impact of the state monopoly on the use of force on law).

158 See for examples Symeon C. Symeonides, *Codifying Choice of Law Around the World* (Oxford University Press 2014), 191–192.

159 See for examples *Id.*, 187–188.

160 Wilke (n 46), 7; Giesela Rühl, "Private international law, foundations," in Giesela Rühl et al. (eds), *Encyclopedia of Private International Law* (Edward Elgar 2017), 1387.

of laws. Insofar as only one legal system provides express rules on property or property-like rights in crypto assets, and this legal system considers its own rules to be applicable in the respective case, the closest connection exists with this legal system. This is because – irrespective of whether the parties could foresee in the individual case this legal system would be applicable – it is also in the interest of the parties and of commerce in general for the facts of the case to be subject to some form of regulation. If several legal systems claim to regulate the respective facts, it must be determined based on an analysis of all the circumstances of the individual case to which law the facts are most closely connected.

3.2.5 The Characterisation of Crypto Assets as Securities

Crypto assets may also be classified as securities within the meaning of the national conflict-of-laws rules.[161] However, a generally valid answer as to whether crypto assets are to be classified as securities in this sense cannot be given. Instead, this depends on how the respective crypto assets are designed in detail and on the concept of securities under the respective national substantive law and conflict-of-laws rules.

In principle, for the determination of the law applicable to securities – irrespective of the requirements for the existence of a security at the level of the substantive law – the law applicable to the right represented by the security and the law governing the legal position in the security itself have to be distinguished.[162] The law applicable to the right underlying the security also determines whether the right can be securitised.[163] For this distinction, it is immaterial whether the security exists in the form of a physical document, the transfer of which is governed by principles of property law, or in the form of a mere register entry, which is transferred by means of a change of entry into the register.[164] Determining the law applicable to the security by using the law

161 For the different understanding of what is meant by a security in the various legal systems, the consequences arising from such a different understanding, and the effects on the national conflict of laws, see Changmin Chun, *Cross-Border Transactions of Intermediated Securites* (Springer 2012), 10–21.

162 From an English perspective, see Hill and Shúilleabháin (n 147), para. 9.5, from a German perspective see Wendehorst (n 142), para. 200.

163 See *e.g.*, for English law Lord Collins of Mapesbury and Harris (n 45), vol. 1, paras. 22-041, 22-044-045; see *e.g.*, for German law Wendehorst (n 142), paras. 200–201.

164 Herbert Kronke and Jens Haubold, "Wertpapierhandels- und Übernahmerecht" in Herbert Kronke, Werner Melis, and Hans Kuhn (eds), *Handbuch Internationales Wirtschaftsrecht* (2nd edn, Otto Schmidt 2017), paras. 185–196; Lord Collins of Mapesbury and Harris (n 45), vol. 1, para. 22-044; Peter Hay et al. (n 143), § 19.32; regarding the Hague Securities Convention, see Roy Goode et al., "Explanatory Report on the Hague Convention on the Law

applicable to the underlying right itself seems uncontroversial. There are, conversely, different approaches to the question of which law governs the property or property-like claims to the security.[165]

Regarding the question of whether crypto assets can be classified as securities, it is decisive that both the conflict of laws and the law applicable to the right underlying the crypto asset classify crypto assets as securities. However, the characterisation of crypto assets as securities is handled very differently and is highly controversial in the various individual legal systems, and, moreover, depends regularly on the type of the crypto asset in question. Legal systems treat securities very differently, even at the level of substantive law. In some jurisdictions, the security is understood as a two-part legal concept in which there is a paper – possibly only a fictitious one – certifying a right. The classification as a security follows from the ownership of the securitised right stemming from the ownership of the paper. In other legal systems, the right does not require an underlying corporeal; instead, it is established and transferred through entries in an intermediary's account.[166] The term "right" is to be understood here in a non-technical sense, *i.e.*, it is not necessary under all legal systems for the right underlying the crypto asset to give rise to further claims against the issuer.[167]

Due to the stark differences, it is impossible to make a general statement about the characterisation of crypto assets. There is a tendency against classifying native crypto assets as securities.[168] In the United States, however, even this general trend is now controversial.[169] In any case, the fungibility of a crypto asset has no influence on its classification as a security. To determine whether crypto assets are to be characterised as securities, the classification by the relevant conflict-of-laws system as well as the law applicable to the securitised right will have to be examined in each individual case.

Applicable to Certain Rights in Respect of Securities held with an Intermediary (Hague Securities Convention)" (HCCH, 2017) I-1 <https://assets.hcch.net/docs/d1513ec4-0c72-483b-8706-85d2719c11c5.pdf> accessed 30 June 2023.

165 Herbert Kronke, *Capital Markets and Conflict of Laws* (Brill 2001), 320 *et seq.*; Chun (n 161), 424.

166 See generally Matthias Lehmann, "Financial instruments," in Jürgen Basedow, Giesela Rühl, and Pedro De Miguel Asensio (eds), *Encyclopedia of Private International Law* (Edward Elgar 2017), 740–741.

167 This applies, for example, to the USA, where the classification of currency tokens, which do not embody any further claims, as securities is disputed, *cf.* Thomas Lee Hazen, "Tulips, Oranges, Worms, and Coins – Virtual, Digital, or Crypto Currency and the Securities Laws" (2019) 20 North Carolina Journal of Law & Technology 493.

168 Hacker and Thomale (n 17), 659–687.

169 Hazen (n 167), 508–513.

3.2.6 The Characterisation of Crypto Assets as Currency

If crypto assets are used in contractual relations as remuneration, they could have the function of a currency for the purposes of conflict of laws. A currency in the conflict-of-laws sense is a means of payment issued by a state.[170]

To determine the law governing questions relating to currency, there are special conflict-of-laws rules of international monetary law. International monetary law distinguishes between the *lex monetae* on the one hand and the currency of debt and payment on the other.[171] The *lex monetae* governs all questions concerning the currency of a state. It determines the permissible legal means of payment, their value, and the monetary units necessary to redeem a debt.[172] The currency of debt determines the value and the amount of the debt. The currency of payment determines the currency in which a payment is to be made.[173] While the distinction between the *lex monetae* and all other issues arising in connection with currencies as the subject of debt relationships is well established, there are differences in the precise categorisation of the latter group of categories. However, here, the specific classification can be left open since there is agreement on the questions of monetary law which cannot be answered with the help of the *lex monetae* being subject to the *lex causae* of the obligation.[174]

Lex monetae is the law of the state whose currency is in question. It is generally accepted that every state is entitled to enact monetary legislation but may not interfere with foreign currencies. Whether a means of payment is legally recognised is determined by the public law of the state whose currency is at stake.[175] The determination of the *lex monetae* for crypto assets is difficult, as these are normally not issued by states. An exception applies only to crypto assets issued by a sovereign state, such as the Venezuelan petro-dollar, or

---

170 Caroline Kleiner, "Money and currency," in Jürgen Basedow, Giesela Rühl, and Pedro De Miguel Asensio (eds), *Encyclopedia of Private International Law* (Edward Elgar 2017), 1255.

171 Ulrich Magnus, "Art 12 Rom I-VO" in Ulrich Magnus (ed), *J. von Staudingers Kommentar zum Bürgerlichen Gesetzbuch: Internationales Vertragsrecht I* (Sellier/de Gruyter 2016), para 102.

172 Charles Proctor, *Mann on the Legal Aspect of Money* (7th edn, Oxford University Press 2012), para 13.04; G. van Hecke, "Currency," in Kurt Lipstein (ed), *International Encyclopedia of Comparative Law Volume III Private International Law* (J.C.B. Mohr, Mouton, and Oceana 1976), 4; on the acceptance of the *lex monetae* principle in the different legal orders see also Proctor (n 172), para. 13.07.

173 Lord Collins of Mapesbury and Harris (n 45), vol. 1, para. 37-004.

174 Proctor (n 172), paras 4.17, 5.33, 7.75, 13.09–13.10; in contrast, the law at the place where the performance is to be rendered is of no particular importance, see Proctor (n 172), para. 4.19.

175 Lord Collins of Mapesbury and Harris (n 45), vol. 1, paras. 37-009–37-010.

blockchain-driven central bank digital currencies currently under discussion in many states.[176] In all other cases, crypto assets cannot be attributed to a state, regardless of their characterisation as a currency. Thus, a *lex monetae* for situations in which they are used as payment cannot usually be determined.[177]

The effects of the lack of a *lex monetae* applicable to crypto assets should not, however, be overestimated. With crypto assets, the regulations to be made by the *lex monetae* are achieved not by legal means but instead by technical means by programming the blockchain appropriately. Also, by agreeing on crypto assets as the means of payments, the parties have just expressed their intention not to be subject to a *lex monetae*. If the sole issue is the use of crypto assets as a means of payment between private individuals, there is also no need for a legal regulation of crypto assets. The regulation already results directly and mandatorily from the program code of the respective blockchain protocol, which is fundamentally resistant to change. In contrast to the other legal questions raised, the subject matter of the *lex monetae* also describes the minimum requirements to be specified in the program code of each blockchain for transactions on the blockchain to be possible from a technical perspective. The units, subunits, and the content of the currency are determined by the code.

Besides the *lex monetae*, international monetary law also governs several questions that are not currency specific. These questions are part of the general references of Article 12 of the Rome I Regulation and Article 15 of the Rome II Regulation, which subject them to the law applicable to the contractual or non-contractional relations as determined by the general rules of these regulations.[178] All questions that are part of international monetary law but outside the *lex monetae* can therefore also be answered for crypto assets with recourse to the general rules.[179] In this respect, according to Article 12(2) of the Rome I Regulation, the law at the place of performance must also be taken into account.[180] State regulations at the place of the deciding court, or the place of

176 See on this *e.g.*, Bank for International Settlements, "Committee on Payments and Market Infrastructures, Markets Committee, Central bank digital currencies" (*Bank for International Settlements*, March 2018) <https://www.bis.org/cpmi/publ/d174.pdf> accessed 30 June 2023.

177 Dickinson (n 56), para. 5.76.

178 *Id*. at para. 5.77; Ulrich Magnus, "Art 12 Rome I" in Ulrich Magnus and Peter Mankowski (eds), *European Commentaries on Private International Law Volume II Rome I Regulation* (Otto Schmidt 2016), para. 47.

179 On the classification of cryptocurrencies and tokens as currency in detail from an English perspective, see Dickinson (n 56), para. 5.74 *et seq*.

180 Proctor (n 172), paras. 4.18–4.20.

performance, which prohibit the use of crypto assets as a means of payment may also become relevant as an overriding mandatory rule.[181]

3.2.7 The Characterisation of Crypto Assets in Insolvency and Succession

Finally, the classification of crypto assets for the determination of the applicable law may also become relevant if a legal transaction covers the entire property of a natural or legal person and the law applicable to this legal transaction is to be determined. Such a situation occurs, for example, in the case of insolvency or inheritance. For the Member States of the European Union, the relevant law is in this respect primarily[182] determined based on the Succession Regulation[183] and the Insolvency Regulation.[184]

If the applicable law is to be determined for a legal transaction relating to the entire estate, in general, the location of individual assets cannot be used to determine the applicable law. According to the Succession Regulation, the applicable law of succession is determined independently of the legal nature of the individual assets of the deceased. Rather, the Succession Regulation links the applicable law of succession to the choice of law or the habitual residence of the deceased (Articles 21 and 22 of the Succession Regulation). A special classification of individual assets, and specifically crypto assets, is therefore not required. The precise legal characterisation of crypto assets is also irrelevant for the determination of international jurisdiction under the Succession Regulation. In this respect, the location of individual assets is partly considered. According to Article 10(2) of the Succession Regulation, the courts of the state in which assets of the estate are located have international jurisdiction if international jurisdiction cannot be established according to Articles 4–9 and 10(1) of the Succession Regulation. However, crypto assets can be subsumed

181 See Article 9 of the Rome I Regulation; Proctor (n 172), paras. 4.24–4.29.

182 Only Denmark and Ireland do not participate in the Succession Regulation; Angelo Davì, "Introduction," in Alfonso-Luis Calvo Caravaca, Angelo Davì, and Heinz-Peter Mansel (eds), *The EU Succession Regulation* (Cambridge University Press 2016), para. 12. The European Insolvency Regulation, on the other hand, applies in all states of the European Union except Denmark; Moritz Brinkmann, "Art. 1," in Moritz Brinkmann (ed), *European Insolvency Regulation* (C.H. Beck, Hart, and Nomos 2019), para. 28.

183 Regulation (EU) No 650/2012 of the European Parliament and of the Council of 4 July 2012 on jurisdiction, applicable law, recognition and enforcement of decisions and acceptance and enforcement of authentic instruments in matters of succession and on the creation of a European Certificate of Succession [2012] OJ L201/107.

184 Regulation (EU) 2015/848 of the European Parliament and of the Council of 20 May 2015 on insolvency proceedings [2015] OJ L141/19.

under Article 10(2) of the Succession Regulation due to the broad concept of assets belonging to the estate.

In contrast, the situation is somewhat different with the Insolvency Regulation. According to Articles 7(1) and 3(1) of the Insolvency Regulation, the applicable law is determined based on the debtor's centre of main interest (COMI), *i.e.*, the legal nature or the location of individual assets are, in principle, irrelevant. The COMI for natural persons is presumed to be the place of the principal place of business (Article 3(1)(3) of the Insolvency Regulation, first sentence) or the habitual residence (Article 3(1)(4) of the Insolvency Regulation, first sentence) of the debtor. Contrary to Recital 30 of the Insolvency Regulation, this presumption is not always rebutted by the mere location of a significant asset in another state.[185] Even in cases where crypto assets constitute a substantial part of the debtor's property, their location by itself is generally irrelevant. Once the law applicable to the insolvency proceedings has been determined pursuant to Article 3(1) of the Insolvency Regulation, according to Article 7(2)(b) of the Insolvency Regulation, this law also determines how crypto assets are to be classified for the purposes of the insolvency proceedings. A separate identification of the law applicable to the determination of the legal nature of the crypto asset is therefore unnecessary.

By contrast, pursuant to Article 8(1) of the Insolvency Regulation, the Insolvency Regulation excludes rights *in rem* of creditors or third parties, with respect to tangible or intangible, movable or immovable assets which are situated within the territory of another Member State at the time of the opening of proceedings, from the law applicable to the insolvency proceedings according to Article 7(1) of the Insolvency Regulation.[186] If rights in crypto assets were to qualify as rights *in rem*, the law applicable to them would have to be determined separately when the crypto asset is located in another state. In this sense, the existence of a right *in rem* in a crypto asset is not ruled out simply because the acquisition of ownership of a crypto asset is currently only possible in a few countries. The concept of rights *in rem* is to be understood autonomously.[187] The term right *in rem*, however, is not defined in the Insolvency Regulation. Such a definition was deliberately omitted, as an autonomous definition would have been accompanied by the risk of the classification as a right *in rem* being assessed differently under the law of the state where the asset is

185 CJEU Case C-253/19 *MH, NI v OJ, Novo Banco SA* [2020] ECLI:EU:C:2020:585, paras. 26–27.

186 Michael Dahl and Justus Kortleben, "Art. 8," in Moritz Brinkmann (ed), *European Insolvency Regulation* (C.H. Beck, Hart, and Nomos 2019), para. 2.

187 See above 3.2.2.2.

located and the Insolvency Regulation.[188] The classification as a right *in rem* within the meaning of the Insolvency Regulation must therefore be made for each individual case by way of interpretation.

Therefore, to ensure a common understanding of the national law where the crypto asset is located and the Insolvency Regulation, the categorisation of the right *in rem* initially depends on the national law of the place where the crypto asset is located. If, according to this law, the right to the crypto asset is to be classified as a right *in rem*, it must be examined whether this right also meets the prerequisites of Article 8 of the Insolvency Regulation, for which the framework set by Article 8(2)-(3) of the Insolvency Regulation is determinative.[189] This requires the right to have a direct and immediate connection with the asset or claim and to be enforceable against all third parties.[190] Thus, depending on the specific design of the right to the crypto asset, it may also be a right *in rem* within the meaning of Article 8(1) of the Insolvency Regulation and crypto assets may therefore be subject to Article 8(1) of the Insolvency Regulation.

4 Conclusion

It thus remains to be said: even though the blockchain and crypto assets implemented on the blockchain are still a fairly recent phenomenon, the crypto asset ecosystem is already saturated with a multitude of different crypto assets with many diverse properties. Depending on the perspective from which crypto assets are to be viewed, there are very different taxonomies in terms of their scope and the type of criteria used. In this context, it is important to remember that the most appropriate taxonomy cannot be determined universally but depends to a large extent on the individual circumstances. For PIL, it has been shown that a taxonomy should be used which is as rudimentary as feasibly possible, with as few differentiation criteria as necessary, but which still reflects the different legal assessments. In this respect, suitable differentiation criteria are fungibility and the representation of assets located off the blockchain.

188 Miguel Virgós and Etienne Schmit, "Report on the Convention on Insolvency Proceedings," para. 100, reprinted in Reinhard Bork and Kristin van Zwieten (eds), *Commentary on the European Insolvency Regulation* (Oxford University Press 2016), 817 *et seq*.

189 Dahl and Kortleben (n 186), paras. 8–16.

190 Virgós and Schmit (n 188), para. 103, reprinted in Reinhard Bork and Kristin van Zwieten (eds), *Commentary on the European Insolvency Regulation* (Oxford University Press 2016), 817 *et seq*.

Regarding the characterisation of crypto assets, it has become clear that in most systems, only very few if any PIL rules at all specifically address crypto assets. However, such specialised PIL rules are not necessary. PIL rules regularly determine the applicable law independently of the object of regulation. Also, the connecting factor of the respective PIL rule can be regularly determined for situations involving crypto assets. Thus, crypto assets do not regularly pose a particular challenge to the existing PIL at the level of characterisation. Rather, difficulties may arise when determining which law the connecting factor of the conflict-of-laws rule declares applicable to crypto assets or which court has international jurisdiction.[191] In particular, it is difficult to determine the competent court or applicable law if the connecting factor of the PIL rule identifies the competent court or applicable law depending on the location of the crypto asset. Whether these difficulties require the creation of specialised PIL rules for crypto assets or whether the existing body of PIL rules is sufficient, only time will tell. So far, the PIL has shown that it also provides appropriate results for phenomena such as blockchain and crypto assets, which the legislator did not have in mind when creating the respective rules.

191 See on this question the following chapters.

CHAPTER 8

Crypto Assets and Decentralised Ledgers: Does Situs Actually Matter?

Amy Held

1 Preliminary Matters

Most, if not all, systems of Private International Law (PIL) reserve special positions for the *lex loci rei sitae* (*lex situs*) and the *forum loci rei sitae* (*forum situs*) in cross-border disputes involving property. For example, all present and former Member States of the EU[1] hold that rights *in rem* relating to immovable property are governed by the *lex situs*; and that the *forum situs* has exclusive jurisdiction to determine the claim. Similarly, when determining whether a thing is immovable or movable, courts around the world consistently depart from the general rule that the *lex fori* governs matters of characterisation;[2] and, instead, apply the *lex situs* of the thing in question.[3]

1 Eva-Maria Kieninger, "Immoveable Property," in Jürgen Basedow et al. (eds), *Encyclopedia of Private International Law Vol 2 Entries I-Z* (Cheltenham: Edward Elgar Publishing 2017), 890–891.

2 Stefania Bariatti, "Classification (Characterisation)," in Jürgen Basedow et al. (eds), *Encyclopedia of Private International Law Vol 1 Entries A-H* (Cheltenham: Edward Elgar Publishing 2017), 357. Bariatti notes that, of the two principal theories for characterisation, the prevailing generally trend favours the application of the *lex fori* over the *lex causae*. Compare the difference in property disputes: Louis d'Avout notes that "in the interests of encouraging international harmony today's judges […] can characterise claims to title in property under the lex situs, despite the fact that the lex fori generally applies to characterisation in international matters." Louis d'Avout "Property and Proprietary Rights," in Jürgen Basedow et al. (eds), *Encyclopedia of Private International Law Vol 2 Entries I-Z* (Cheltenham: Edward Elgar Publishing 2017), 1429.

3 Kieninger (n 1), 893. Kieninger notes that in some EU jurisdictions, such as Lithuania and the Netherlands, the application of the *lex situs* to characterisation is expressly spelled out; in others, the same result is achieved by the general application of the *lex situs* rule. In England, the position has been set out in the following terms: "If there is a conflict between the lex situs and the lex fori as to whether a particular thing is movable or immovable, it is well settled that the lex situs at the decisive moment must control" in Lord Collins of Mapesbury and Jonathan Harris (eds), *Dicey, Morris, and Collins on the Conflict of Laws* (15th edn, London: Sweet & Maxwell 2012), para. 22-009 (fn 16 and text) ("*Dicey, Morris, and Collins*"). It has,

© AMY HELD, 2023 | DOI:10.1163/9789004514850_010
This is an open access chapter distributed under the terms of the CC BY-NC-ND 4.0 license.

Such degree of consensus is, on the one hand, remarkable in PIL; *a fortiori* in an area of law in which, perhaps, the widest degree of divergence amongst jurisdictions may be seen. On the other hand, such consensus may be unsurprising, considering the origins of the *lex* and *forum situs* rules in ancient customary laws premised upon the territorial sovereignty of a nation state.[4]

Notwithstanding, however, an increasingly interconnected, globalised world, traditional concepts of territoriality remain very much at the heart of the modern rules of PIL. The traditional approach of the common law asserts 'exorbitant' jurisdiction over any and all persons physically present on the territory of England, howsoever fleeting or by chance happenstance. The modern rules of jurisdiction under the English Civil Procedure Rules 1998 (CPR) may well have seen a shift in emphasis from physical presence within the jurisdiction to the legal service of process; nevertheless, the methods prescribed by the CPR for such service remain premised on presence within the jurisdiction as the default rule.[5] Only where a defendant is without the territorial jurisdiction of England do considerations unrelated to territorial sovereignty – such as the merits of the proposed claim or *forum conveniens* – play any role in establishing the jurisdiction of the English courts.

Concepts of territoriality continue to resonate also in contemporary justifications for the primacy of the rules referring to *situs*. Modern adherents to Savignian theory take as a logical starting point that "the *res* is the object of a connecting rule and that it cannot be assigned to a non-territorial regime."[6] The *Jenard* Report[7] to the Brussels Convention, by contrast, includes one

---

however, been also noted that the application of lex situs to matters of characterization has been criticized by scholars; see d'Avout (n 2), 1429.

4 Typical justifications grounded in Westphalian concepts of sovereignty include the public interest considerations inherent in courts applying their own local law to all things – particularly land – within its territorial jurisdiction; see, for example, d'Avout (n 2), 1428 et seq. A tempering of such position on the basis of party autonomy may be seen in Savigny, who was of the view that "he who wishes to acquire, to have, to exercise a right to a thing, goes for that purpose to its locality, and voluntarily submits himself, as to this particular legal relation, to the local law that governs in that region." Friedrich Karl von Savigny, *A Treatise on the Conflict of Laws* (2nd edn, Edinburgh: T&T Clark 1869) (translated by William Guthrie), 129, as cited in Janeen M Carruthers, *The Transfer of Property in the Conflict of Laws: Choice of Law Rules in Inter Vivos Transfers of Property* (Oxford: OUP 2005), para. 8.13.

5 Pursuant to CPR Rule 6.6, the claim form must be served within the jurisdiction, except where CPR Rule 6.7(2) (solicitors in Scotland or Northern Ireland), CPR Rule 6.11 (service by a contractually agreed method), or CPR Rule 6.36 (service out of the jurisdiction) apply.

6 d'Avout (n 2), 1428.

7 "Report by Mr P. Jenard on the Convention of 27 September 1968 on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters," [1979] OJ C59/1 ("the Jenard Report").

unusually pragmatic justification for the decision to confer exclusive jurisdiction on the *forum situs* in disputes relating to immovables: promotion of the free circulation of judgments within the EU.[8] Other, more familiar, territorial justifications included in the Report are: (i) the need to conduct on-the-spot checks, enquiries, and expert examinations during the course of litigation; (ii) the *forum situs* being best placed to apply the customary practices that will often, at least in part, govern the matter; and (iii) the need to make entries in land registers located where the property is situated.[9] As has been recognised,[10] these considerations reflect choice of law rather than jurisdiction; and, indeed, *lex situs* is typically selected as governing law for actions *in rem*.

The arguments for the application of the *lex situs* in respect of movables tend to revolve around two principal themes: (i) as with immovables, practical control over the asset in question and the potential for unenforceable judgments in conflict with the *lex situs*;[11] and (ii) commercial considerations – relating primarily to certainty and security of acquisition by third party creditors or purchasers – require an objective and easily ascertainable connecting factor for the benefit of third parties.[12] More generally, modern arguments for the *lex*

8 *Id*., 35. As a matter of national law, several Member States – notably Germany and Italy – expressly conferred exclusive jurisdiction on those courts on grounds of public policy. As such, in the absence of a rule of exclusive jurisdiction, judgments given by courts in other Member States on different bases of jurisdiction – for example, the defendant's domicile, or an agreed forum – would not be recognised nor enforced in those first Member States.

9 *Id*.

10 Geert van Calster, *European Private International Law: Commercial Litigation in the EU* (3rd edn, Oxford: Hart 2021), para. 2.162.

11 For example, in *Glencore International AG v Metro Trading International Inc* (*No.2*) [2001] 1 All ER (Comm) 103; [2001] 1 Lloyd's Rep 344, paras. 31–32 (Moore-Bicke J): "[…] Practical control over movables can ultimately only be regulated and protected by the state in which they are situated and the adoption of the lex situs rule in relation to the passing of property is in part a recognition of that fact. That is just as much true in relation to the passing of property between the parties to the transaction as it is in relation to the passing of property between one or other of them and a third party. Some recognition of the practical control exercised by the state in which goods are situated is no doubt reflected in the expectation that a transaction which would be effective by the law of that state to pass a good title will in fact do so. These considerations together with the practical considerations of trade and commerce provide strong support in my view for the adoption of a lex situs rule in all cases. […]".

12 *Dicey, Morris, and Collins* (n 3), para. 22-025. Consider also: *Re Anziani, Herbert v Christopherson* [1930] 1 Ch 407, 420 (Maugham J) "I do not think that anybody can doubt that. With regard to the transfer of goods, the law applicable must be the law of the country where the moveable is situate. Business could not be otherwise;" and *Macmillan Inc v Bishopgate Investment Trust plc* (*No 3*) [1996] 1 WLR 387, 399 (Staughton LJ) "a purchaser ought to satisfy himself that he obtains a good title by the law prevailing where the chattel

situs include ease of application; simplicity and neutrality;[13] and consistency of principle.[14]

Situs, thus, occupies a unique position in PIL as a connecting factor. Such position has driven one commentator to conclude that:

> [*lex situs*] triumphantly has withstood the climate of change, and which remains largely the same, and as apparently invincible, as it was in the early years of the twentieth century, and before. Certainly as regards the transfer of immovable property, generally as regards the *inter vivos* transfer of tangible movable property, and frequently in the case of the lifetime transfer of intangible movable property, the law of the situs (as defined for each category) has long been considered to be the apposite connecting factor.[15]

Intangible assets are difficult to reconcile with such 'situs monopoly.' By their very nature, such assets are not situate anywhere in any meaningful sense at all. How, then, should courts determine governing law for disputes involving intangibles? Which connecting factor should take precedence? To provide solutions to such questions, legal systems have typically maintained the rules based on *situs* and have, instead, modified the legal concept of intangible assets by ascribing to them an artificial situs.

Thus, in England, simple debts have been held to be situate at the habitual residence of the debtor:[16] ultimate enforcement of the obligation underpinning the chose in action requiring the owner to bring legal proceedings in the courts exercising personal jurisdiction over the defaulting debtor. Bearer instruments, such as bills of exchange and bearer bonds, have simply been

---

is… but should not be required to do more than that And an owner, if he does not wish to be deprived of his property by some eccentric rule of foreign law, can at least do his best to ensure that it does not leave the safety of his own country."

13 Geoffrey Chevalier Cheshire, *Private International Law* (3rd edn, Clarendon Press 1947), 563, cited in Janeen M Carruthers, *The Transfer of Property in the Conflict of Laws: Choice of Law Rules in Inter Vivos Transfers of Property* (Oxford: OUP 2005), para. 8.10 (fn 31): "the lex situs has the great advantage of being a single and exclusive system that, possessing effective control over the subject matter of the suit, can act as an independent arbiter of conflicting claims."

14 *Glencore International AG* (n 11), para. 30: "[c]onsistency of principle requires that the same rule should apply whether or not third party interests are involved."

15 Janeen M Carruthers, *The Transfer of Property in the Conflict of Laws: Choice of Law Rules in Inter Vivos Transfers of Property* (Oxford: OUP 2005), para. 2.06.

16 Rule 129(1) of *Dicey, Morris, and Collins* (n 3); *id.*, paras. 22-026–22-032.

treated as chattels:[17] the underlying obligations distinguished from the physical paper, possession of which confers rights of ownership over those obligations. Registered intangibles, such as registrable shares, have been held to be situate at the place where the register is maintained.[18] In the EU, the same approach has been applied to dematerialised securities held by a financial intermediary, which are deemed situate at the place where the relevant securities account is maintained.[19]

As, however, the computing revolution of the 1990s continues to mature with the advent of decentralised ledger technology, recourse to an artificial *situs* for the intangible products of the 'Fourth Industrial Revolution,' *prima facie*, appears untenable. It is relatively uncontroversial that where rights in intangible assets are recorded on a register, the *situs* of those rights can be ascribed to the place where that register is maintained. In the case of decentralised ledgers, this reasoning cannot apply: to where can the law ascribe *situs* if no 'master' copy exists at all, but a complete and full copy is maintained in real time across a decentralised network of nodes?[20] If such ledgers were originally intended to record the distribution of crypto assets amongst network participants, should a choice-of-law rule apply to both the proprietary and contractual aspects of any acquisition and disposition of crypto assets effected by the network of nodes and recorded on the decentralised ledger?[21] Are crypto assets actually '*choses* in action' or 'claims' to which concepts of assignments properly apply? Are they even subjects of property rights at all? If so, where within the property taxonomy do they belong,[22] and what underlying feature of the asset should be taken as definitive for the purpose of identifying

17 *Id*., paras. 22-040–22-042; hence Rule 129(3) applies.

18 *Id*., para. 22-044 (fn 114).

19 Art. 9(1) of the Directive of the European Parliament and of the Council 2002/47/EC of 6 June 2002 on Financial Collateral Arrangements, [2002] OJ L168/0043; Art. 9(2) of the Directive of the European Parliament and of the Council 98/26/EC of 19 May 1998 on Settlement Finality in Payment and Securities Settlement Systems, [1998] OJ L166/45; Art. 24 of the Directive of the European Parliament and of the Council 2001/24/EC of 4 April 2001 on the Reorganisation and Winding Up of Credit Institutions, [2001] OJ L125/15.

20 Philipp Paech, "The Governance of Blockchain Financial Networks" (2017) 80 Modern Law Review 1073, 1106; Philipp Paech, "The International Law of Crypto-Asset Settlement – Functional Analysis and Draft Legal Principles" (*UNIDROIT*, May 2019) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2792639> accessed 31 May 2022.

21 Paech, "The International Law of Crypto-Asset Settlement – Functional Analysis and Draft Legal Principles" (n 20), 3.

22 Financial Markets Law Committee ("FMLC"), "Issues of Legal Uncertainty Arising in the Context of Virtual Currencies" (*FMLC*, July 2016), 6 *et seq* <http://fmlc.org/report-virtual-currencies-18-july-2016/> accessed 30 June 2023.

a connecting factor? Such questions have caused concern that PIL has found an 'intractable' problem which cannot be circumvented by current legal principles.[23] Accordingly, it was recognised as early as 2017 that "any modernisation of the conflict-of-laws regime should…take due account of distributed ledger technology."[24]

Hence, there has more recently been several proposals for ascribing to crypto assets and/or decentralised ledgers an artificial *situs*. These are briefly considered in turn. A basic knowledge of the code underpinning decentralised ledger technologies is assumed.[25]

Owner. One proposal that has notably been cited at first instance in England and Wales[26] is that of Professor Andrew Dickinson, who suggests that a bitcoin is situate at the place where its owner is domiciled. This proposal is premised on a technical analysis of crypto assets as comprising the "legitimate expectations of participants in a decentralised ledger network that the ledger will attribute particular units of value within the system and the power to deal with those units."[27] Hence, an analogy with business goodwill as a species of intangible property that is situate, for the purpose of the English common law rules referring to *situs*, in the country where the premises to which the goodwill is attached are situate.[28]

The key difficulty, however, with such proposal is that it assumes what is required to be proved: in an outright proprietary dispute between parties as to ownership of certain bitcoin, the owner of the bitcoin in question remains in issue.[29]

---

23 ISDA and Linklaters LLP, "Whitepaper: Smart Contracts and Distributed Ledgers – A Legal Perspective" (*ISDA*, 3 August 2017), 9 <https://lpslive.linklaters.com/en/about-us/news-and-deals/news/2017/smart-contracts-and-distributed-ledger--a-legal-perspective>. See also FMLC, "Distributed Ledger Technology and Governing Law: Issues of Legal Uncertainty" (*FMLC*, 27 March 2018), para. 4.6 <http://fmlc.org/wp-content/uploads/2018/05/dlt_paper.pdf>.

24 Thomas Keijser, "Financial Collateral Arrangements in the European Union: Current State and the Way Forward" (2017) 22 Uniform Law Review 258, 291.

25 Readers unfamiliar with the technology or otherwise needing a refresher are directed to Chapter 10 of this book. A concise account of the author's own may be found at Amy Held, "Private Keys v Blockchains: What *is* a Cryptoasset in Law?" (2020) 4 Journal of International Banking and Financial Law 247.

26 *Ion Science Ltd and Anor v Persons Unknown, Binance Holdings Limited and Payward Limited* (unreported, 21 December 2021); *Fetch.AI Ltd and Anor v Persons Unknown, Binance Holdings Limited, and Binance Markets Limited* [2021] EWHC 2254 (Comm).

27 Andrew Dickinson, "Cryptocurrencies and the Conflict of Laws," in David Fox and Sarah Green (eds), *Cryptocurrencies in Public and Private Law* (Oxford: OUP 2019), para. 5.107.

28 *Id.*, para. 5.108.

29 See further Amy Held, "Does Situs Actually Matter when Ownership to Bitcoin is in Dispute?" 2021 4 Journal of International Banking and Financial Law 269.

Nodes. Associate Professor Philipp Paech's analysis emphasises the decentralised ledger: for the purpose of determining the *lex rei sitae*, the location of the nodes is the relevant connecting factor. Although no justification is given for such propositions, Paech immediately proceeds to reject an artificial *situs* based on the nodes, given that this would lead to the application of different laws within the decentralised ledger network.[30]

Private Key/Transferor. By contrast, the UK Financial Markets Law Committee has identified a potential solution emphasising the private key. Two possibilities for an artificial *situs* stem from such premise: (i) the place where the private key is situate;[31] or (ii) the place where the system participant transferring the crypto asset – using the private key – is resident, or has its centre of main interests, or is domiciled.[32]

The primary difficulty with this approach lies in the nature of the private key itself as a large and unique number generated according to cryptographic standards of randomness. Private keys are, thus, in themselves just as much an intangible concept as the crypto asset itself. Accordingly, any proposed solution to the problem of localising a crypto asset based on the private key merely defers consideration of the issue: where then is the private key situate for the purpose of proposal (i) above? In addition, the ease with which infinite copies of a private key, once generated, may be made poses significant difficulties for identifying which copy is definitive for the purpose of a legally valid transfer. In the absence of a definitive register linking private keys with users, the difficulty in identifying who in fact used a private key to propose a change in state within an unpermissioned network – and whether the law considers that they were entitled to do so – renders proposal (ii) above untenable.

Lex Codicis/Lex Digitalis. Another possibility identified by the Financial Markets Law Committee refers to the code underpinning the decentralised ledger network protocol and suggests that crypto assets may be considered situate at the primary residence of the original coder.

The Financial Markets Law Committee, however, considers that a significant disadvantage of this solution is that it is "difficult to explain why the original coder should impact the ongoing life of the distributed ledger where s/he is not also the system administrator."[33] Another key difficulty would be in identifying the relevant coder: some unpermissioned networks, such as Ethereum, have a publicly acknowledged 'creator'; others, notably Bitcoin, are well-known for the anonymity of the original coder. In the latter case, there have

30 Philipp Paech, "The Governance of Blockchain Financial Networks" (n 20).

31 'FMLC' (n 23), para. 6.23.

32 *Id.*, para. 6.21.

33 *Id.*, para. 6.28.

been many persons come forward as 'Satoshi Nakamoto';[34] which of these – or if none of them, who – the 'original coder' is for the purpose of this proposal remains problematic.

Such proposals are well worth considering, subject to a general caveat: each are premised upon assumptions as to (i) the underlying property characterisation of the asset, both in itself as an empirical phenomenon, and also as translated into the terms of national property laws; and (ii) its particular use case in practice. Such assumptions are important to recognise as there is no consistency in how they are approached by the authors of each proposal, yet shape perceptions as to the most relevant connecting factor to serve as a basis for an artificial *situs*. Accordingly, this contribution will not adopt any overarching property characterisation of crypto assets,[35] but will consider 'crypto assets' as a broad, undefined concept, encompassing the arguably separate things of 'the asset' itself, private keys, and decentralised ledgers. The discussion will also focus on unpermissioned networks, given that permissioned networks pose less of a challenge for the concept of *situs*; the facts of such networks often disclose a familiar connecting factor, such as a central operating authority.

From a broader perspective, it is critical to recognise that implicit in any proposal for an artificial *situs* is the premise that *situs* will and should apply as the relevant connecting factor in cross-border disputes involving crypto assets as subjects of proprietary claims. Given the present focus of this contribution on whether such premise is justified, this Part 1 of the present contribution set out the general justifications advanced for the unique position that *lex situs* and *forum situs* occupy in PIL. Part 2 then considers the extent to which *situs* will not matter in live proceedings before the courts, with reference to decided cases. Part 3 considers the circumstances in which *situs* will indeed matter, by reference to a hypothetical case. Part 4 sets out broader criticism of the '*situs* monopoly,' before offering final conclusions in terms of reform to national property laws, guidance in EU PIL, and a potential international solution addressing the property aspects of crypto assets for the purpose of PIL. The contribution will focus on the position under the common law of England and Wales (which, for the sake of convenience, will be referred to simply as

34 See, for example, *Crypto Open Patent Alliance v Wright* [2021] EWHC 3440 (Ch), where the relief sought was a declaration that the Defendant is not Satoshi Nakamoto.

35 The author's own property analyses may be found in Held (n 25); Amy Held, "Intermediated Cryptos: What Your Crypto Wallet *Really* Holds" (2020) 8 Journal of International Banking and Financial Law 540; Amy Held, "Baking, Staking, Tezos, and Trusts: Crypto Sale and Repurchase Agreements Analysed by the High Court" (2022) 2 Journal of International Banking and Financial Law 96.

'England'); and the EU regime set out in the Brussels I Recast Regulation, Rome I Regulation, and Rome II Regulation.

2 When *Situs* Won't Matter

Notwithstanding the extent to which rules referring to *situs* are entrenched in PIL systems, the assumption that all and any disputes involving crypto assets will necessarily involve an exercise in localising the asset undermines the function and effect of initial characterisation by the courts.

2.1 *Characterisation*

Characterisation is a fundamental aspect of PIL that "results from the fact that the rules which have evolved to deal with choice-of-law problems are expressed in terms of juridical concepts or categories and localising elements or connecting factors."[36] Hence, it has been described in England as "a doctrine which is an essential part of the mechanism by which a court chooses which law to apply in cases in which the framework for the decision and the rules for choice of law are those of the common law."[37] Characterisation is, thus, often associated with determining the *lex causae*, sequentially relevant only after the court has first satisfied itself that it has jurisdiction.[38] In practice, however, characterisation is also relevant at the earlier stage of establishing jurisdiction, and the decided cases demonstrate the extent to which the question of characterisation for this purpose may indirectly raise the issue of where a crypto asset is situate.

Characterisation, at least in non-proprietary disputes, is typically a matter determined according to the *lex fori*, and the classic statement of the way in which the English courts approach characterisation is found in *Macmillan Inc v Bishopgate Investment Trust Plc* (*No 3*): "…the proper approach is to look beyond the formulation of the claim and to identify according to the *lex fori* the true issue or issues thrown up by the claim and defence."[39] In that case, the Claimant ('Macmillan') asserted a beneficial interest in shares provided by their nominee as security on certain loans made to him personally in breach of trust, which ultimately were transferred to the Defendant Banks. Macmillan

36 *Dicey, Morris, and Collins* (n 3), para. 2-002.
37 *Dicey, Morris, and Collins* (n 3), para. 2-006.
38 Paul Torremans et al. (eds), *Cheshire, North & Fawcett*: *Private International Law* (15th edn, Oxford: OUP 2017), 41.
39 *Macmillan Inc* (n 12), 407B (Auld LJ).

accordingly sought various declarations that it was beneficially entitled to the shares and that the Banks held them on constructive trust for Macmillan. It also sought orders for restoring the shares to Macmillan and compensation and/or damages for breach of constructive trust and/or conversion.

In respect of the characterisation issue before the court, Macmillan submitted that its claim was essentially one for restitution. The Banks, on the other hand, pleaded that they had acquired title to the shares in good faith and for value, without notice of Macmillan's beneficial interest. Accordingly, the Banks characterised the issue as one of priority between proprietary interests in the shares. Staughton LJ found for the Banks on the issue: the rules of conflict of laws were to be directed to the particular issue of law in dispute, rather than at the cause of action upon which the claimant relied. It was, thus, the Defence that identified the relevant issue, namely, whether in law the Banks were purchasers for value in good faith without notice, so as to obtain good title to the shares.[40]

Thus, determinations of the *lex causae* – and in appropriate cases, jurisdiction – will, in practice, be heavily influenced by the factual context within which a legal dispute arises as the premises informing both the pleadings and the exercise in legal characterisation undertaken by the court. Accordingly, the importance of maintaining a pragmatic approach can hardly be overstated. Relevant considerations in disputes involving crypto assets will include the typical ways in which end-users deal and transact in crypto assets; the commercial practices in effecting such dealings and transactions; and the ways in which crypto assets generate demand amongst the general public as a valued resource. One particularly salient factor is that direct participation by individual users in a given decentralised ledger network is rare; even in the case of native crypto assets in an unpermissioned network, most holdings of crypto assets are partially, if not wholly, intermediated through a vast range of intermediaries, such as exchanges, wallet providers, and key custodians.

That the legal relationships between the parties and the nature of their commercial agreements can have significant bearing on the pleadings, characterisation, and, ultimately the relevance of *situs* as a connecting factor, is best illustrated, however, by reference to case studies.

2.2 E v A*: Contracts*

In *E v A,*[41] a German domiciliary wished to acquire a holding in a cryptocurrency investment marketed by an Austrian entrepreneur, which could only be

40 *Id*., 398H-399C (Staughton LJ).

41 *E v A*, ZFR 2021/101 S 250 (Diwok), Decision of 4 November 2020. <https://www.ris.bka.gv.at/Dokumente/Justiz/JJT_20201104_OGH0002_0030OB00095_20X0000_000/JJT_20201104_OGH0002_0030OB00095_20X0000_000.html> accessed 30 June 2023.

paid for in bitcoin. When, however, the parties tried to effect the payment, the Austrian entrepreneur's bitcoin 'ATM' malfunctioned. Accordingly, the parties agreed that the Austrian entrepreneur would acquire the investment in his own name using 6 bitcoin held in his own cryptocurrency wallet. The 6 bitcoin would then be reimbursed by the German domiciliary within a month in exchange for the participation in the investment. When the German domiciliary declined to pay, the Austrian entrepreneur brought proceedings in the Austrian courts, which characterised the dispute as a 'contract of exchange' within the meaning of the relevant provisions of both the Austrian and German Civil Codes. Accordingly, pursuant to Article 7(1)(a) of the Brussels I Recast Regulation, the subject of the exercise in localisation was not the bitcoin, but the place of performance of the contractual obligation in question. This was held to be Germany, as the place where the debtor in the exchange was domiciled. Hence, the Austrian courts at first instance and on first appeal declined jurisdiction in favour of the German courts.

E v A is a useful reminder of the extent to which the existence of a contract will often obviate the need for any proprietary analysis, let alone a localisation of the crypto asset in dispute. Irrespective of whether or not the parties are aware of the legal consequences of their actions and agreements, or whether the crypto asset is used as consideration or is the subject of the exchange itself, the fact that the dispute concerns a crypto asset will often be irrelevant to the question of characterisation. In *E v A* itself, the outcome would have been the same if the agreement had not concerned crypto assets at all: if the German domiciliary's obligation to reimburse were denominated in fiat currency, rather than in bitcoin, the exercise in localisation would still have proceeded under the same rules, which ultimately point to the debtor's domicile. An alternative characterisation of the transaction as a loan[42] further emphasises the importance of the underlying agreement, rather than its subject matter: loan contracts are governed by Article 7(1)(b) of the Brussels Recast Regulation, and the subject of the exercise in localisation again refers to the place of performance of the contractual obligation in question. Under the case law of the CJEU, such place of performance of a long-term loan is where the lender has its domicile;[43] again, the fact that the loan might be of 6 bitcoin rather than some other asset does not change this analysis. It is, therefore, unsurprising

42 Many thanks to Matthias Lehmann for sharing this case with me. His comment on this case and observations on the loan characterisation, upon which I have drawn, may be found in Matthias Lehmann, "Bitcoin Trades and Consumer Jurisdiction" (*EAPIL*, 29 January 2021) <https://eapil.org/2021/01/29/bitcoin-trades-and-consumer-jurisdiction/>.

43 Judgment of the Court (Third Chamber) of 15 June 2017, *Kareda v Benkö*, [2017] OJ C277/16, Case C-249/16.

that the Austrian courts focused on the transaction and commercial agreements between the parties, rather than the *subject* of those transactions and agreements.

It is submitted that such cases underpinned by a contract are likely to be the norm, rather than the exception, given: (i) the original and continued use of crypto assets as a means of exchange; (ii) the concentration of second generation use cases in the financial markets and investment contexts; and (iii) the highly intermediated nature of the crypto asset market. In these cases, the commercial context will have considerable impact on the exercise in characterisation, which will then proceed on the familiar principles and connecting factors applicable to contracts, rather than those applicable to property. As will be shown, however, this does not necessarily mean that localisation will not feature whatsoever in the analysis.

To analyse the position in contract, it is worth distinguishing two types of cases: (i) cases in which the parties have made an express choice of governing law and/or of jurisdiction; and, (ii) cases in which the parties have not. Finally, given the prevalence of intermediaries in the crypto asset market, it will also be worth considering (iii) consumer contracts.

2.2.1 Governing Law and Jurisdiction Clauses

As crypto assets become increasingly accepted in mainstream commerce as a means of payment, it is likely that the underlying transactions will be made pursuant to formal, written contracts drafted with the benefit of legal advice. Many such contracts will contain an express jurisdiction and/or governing law clause.

For example, in June 2021, the international auction house, Christie's, announced that, in the forthcoming auction of an untitled Keith Haring painting valued at GBP 3.9 million,[44] payments in bitcoin or ether would be accepted as alternatives to fiat currency. The 'Post Lot Text' to the listing is supported by a clear jurisdiction and governing law clause contained in the Standard Conditions of Sale (Figure 8.1).

Similarly, the User Agreements for two popular crypto exchanges, hosted by the Gemini Trust Company LLC (Gemini) and Coinbase Europe Limited

44 Keith Gill, "Property From a Distinguished Private European Collection: Keith Haring (1958–1990) Untitled" (*Christie's*, 30 June 2021), Lot 23 in live auction 20068 <https://www.christies.com/lot/lot-6328194>.

9. LAW AND DISPUTES This agreement, and any contractual or non-contractual dispute arising out of or in connection with this agreement, will be governed by English law. Before either you or we start any court proceedings and if you and we agree, you and we will try to settle the dispute by mediation in accordance with the CEDR Model Mediation Procedure. If the dispute is not settled by mediation, you agree for our benefit that the dispute will be referred to and dealt with exclusively in the English courts; however, we will have the right to bring proceedings against you in any other court.

FIGURE 8.1 Christie's standard conditions of sale (London version), Clause 9[45]

(Coinbase), both expressly include both a jurisdiction/dispute resolution and governing law clause (Figure 8.2 and Figure 8.3).

Inclusion of such clauses have significant consequences for any PIL issues arising in a dispute, as both the English[46] and EU[47] systems recognise and give primacy to the choice of the parties to a contract as to the law applicable to their agreement and their chosen forum for the resolution of disputes. Express jurisdiction and governing law clauses will, therefore, fall squarely to be determined within those provisions of PIL that give effect to party choice in matters of contract. This will, in principle, pre-empt any need for a court to: (i) resort to a proprietary characterisation of the dispute, cause of action, or issue for determination; and (ii) make findings in respect of the *situs* of a crypto asset or a decentralised ledger in order to determine those issues. It is, therefore, pragmatic that the EU Commission's Proposal for a Regulation on Markets in Crypto-Assets includes a requirement that all persons "engaged in the issuance of crypto-assets or provide services related to crypto-assets in the EU"[48] are to include in their "custody and administration agreements" the law applicable

45 Christie's, "London Conditions of Sale: Buying at Christie's" (*Christie's*) <https://www.christies.com/media-library/pdf/conditions-of-sale/london-conditions-of-sale.pdf> accessed 30 June 2023.

46 An exclusive jurisdiction clause designating the English courts entered into on or after 1 October 2015 will generally be given effect in England by Arts 5 and 6 of the Hague Convention of 30 June 2005 on Choice of Court Agreements. As for *lex causae,* see *Whitworth Street Estates* (*Manchester*) *Ltd v James Miller and Partners* Ltd [1970] AC 583, 603 (Lord Reid); *Vita Food Products Inc v Unus Shipping Co Ltd* [1939] AC 277, 299 (PC).

47 Art. 25(1) of the Regulation 1215/2012 of the European Parliament and of the Council on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast), [2012] OJ L351/1 ("Brussels I Recast"); Art. 3(1) and Recital 11 of the Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), [2008] OJ L 177/6 ("Rome I").

48 Art. 2 para. 1 Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM (2020) 593/3 ("MiCA").

This User Agreement, your use of Gemini, your rights and obligations, and all actions contemplated by, arising out of or related to this User Agreement shall be governed by the laws of the State of New York, as if this User Agreement is a contract wholly entered into and wholly performed within the State of New York. YOU AGREE THAT ALL ORDERS, TRADES, DEPOSITS, WITHDRAWALS, OR SALES ON GEMINI AND CONTEMPLATED ACCORDING TO THE TERMS OF THIS USER AGREEMENT SHALL BE DEEMED TO HAVE OCCURRED IN THE STATE OF NEW YORK AND BE SUBJECT TO THE INTERNAL LAWS OF THE STATE OF NEW YORK WITHOUT REGARD TO ITS CONFLICTS OF LAWS PROVISIONS.[49]

Dispute Resolution

You agree and understand that any controversy, claim, or dispute arising out of or relating to this User Agreement or the breach thereof shall be settled solely and exclusively by binding arbitration held in New York, New York, administered by JAMS and conducted in English, rather than in court....

[...]

You agree that you or we may, without inconsistency with this arbitration provision, apply to any court for an order enforcing the arbitral award. You irrevocably and unconditionally agree to waive any objection that you may now or hereafter have to the laying of venue of any action or proceeding relating to enforcement of the arbitral award in the federal or state courts located in the State of New York.

[...]

IF FOR ANY REASON THIS ARBITRATION CLAUSE BECOMES NOT APPLICABLE OR FOR ANY OTHER REASON LITIGATION PROCEEDS IN COURT THEN YOU AGREE THAT YOU AND WE:

TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAWS AND REGULATIONS, HEREBY IRREVOCABLY WAIVE ALL RIGHT TO TRIAL BY JURY AS TO ANY ISSUE RELATING HERETO IN ANY ACTION, PROCEEDING, OR COUNTERCLAIM ARISING OUT OF OR RELATING TO THIS USER AGREEMENT OR ANY OTHER MATTER INVOLVING US HERETO, AND

SUBMIT TO THE EXCLUSIVE JURISDICTION AND VENUE OF THE FEDERAL OR STATE COURTS LOCATED IN NEW YORK COUNTY, NEW YORK AND YOU AGREE NOT TO INSTITUTE ANY SUCH ACTION OR PROCEEDING IN ANY OTHER COURT IN ANY OTHER JURISDICTION.[50]

FIGURE 8.2 Gemini user agreement, governing law and dispute resolution provisions

to the agreement.[51] Should such provision be enacted, it is likely that a large number of disputes concerning crypto assets will not require any recourse to traditional property conflict-of-laws rules referring to *situs*.

49 Gemini, "User Agreement" (*Gemini*, 4 March 2022) <https://www.gemini.com/legal/user-agreement#section-governing-law>.

50 *Id.*

51 *Id.*, Art. 67 subpara. 1(f). The rules on jurisdiction under Brussels I Recast would apply, but given the presence of a central operator, this is unlikely to be problematic.

13.21 Governing Law and Jurisdiction. This Agreement and the relationship between us shall be governed by the laws of Ireland and the non-exclusive jurisdiction of the Irish courts, subject to any local mandatory law, or rights available to Consumers.[52]

FIGURE 8.3 Coinbase user agreement, Clause 13.21

In order to be effective, however, any governing law or jurisdiction clause must comply with the relevant requirements[53] if they are to be upheld by the courts. If, however, a choice of governing law or a dispute resolution clause cannot be enforced, the courts will turn to the provisions applicable in cases where the parties have not made any choice of law.

2.2.2 Absence of Party Choice

Where the parties have not made an express choice of governing law or of forum, it is necessary to distinguish between two types of transactions owing to the way in which certain rules of PIL are framed. First, there are those transactions, such as Christie's auction of the Haring painting, in which the crypto asset is used as an alternative to fiat currency as contractual consideration, *i.e.*, the means through which the payment obligation in exchange for a good or service is discharged, or what was in *E v A* characterised as the 'debt' obligation in a contract of exchange. By contrast, there are those transactions where the crypto asset is, in itself, the subject of the exchange and for which consideration (often in fiat currency) is given. Examples of this latter type of transaction are typically likely to occur at the 'entry' point to the crypto asset sector, such as the initial 'buy in' to a cryptocurrency exchange. Whether the crypto asset is, thus, used as consideration or is, in itself, the subject of exchange will have some bearing on how the relevant contract is localised.

2.2.2.1 *England*

If a proposed defendant is not present within the English territory, English proceedings can only be served legally upon him without the jurisdiction by permission of the court. The test applied upon any such application for

52 Coinbase, "Coinbase User Agreement" (*Coinbase*) <https://www.coinbase.com/legal/user_agreement/ireland_europe> accessed 30 June 2023.

53 In this regard, parties should note the provisions of Art. 25(1) and (2) of the Brussels I Recast (n 50), and Arts. 11, 12, and 13 of Rome I (n 50). Furthermore, requirements regarding the validity of dispute resolution and jurisdiction clauses under national law should be taken into account.

permission to serve out of the jurisdiction, as summarised by the authorities,[54] has three limbs, each of which must be satisfied if permission is to be granted:

1. There is a good arguable case that the claim against the proposed foreign defendant falls within one or more of the heads of jurisdiction – colloquially known as 'Gateways' – for which leave to serve out of the jurisdiction may be given, as set out in paragraph 3.1 of CPR Practice Direction 6B;
2. In relation to the proposed foreign defendant, there is a serious issue to be tried on the merits of the claim; and
3. In all the circumstances, (a) England is clearly or distinctly the appropriate forum for the trial of the dispute ('*forum conveniens*'); and (b) the court ought exercise its discretion to permit service of the proceedings out of the jurisdiction.

In respect of contracts, English courts assert jurisdiction over defendants, wheresoever they are in the world, if the claim concerns a contract made within the jurisdiction or governed by English law (Gateway 6); and claims made in respect of a breach of contract committed within the jurisdiction (Gateway 7).

Jurisdiction under Gateway 6 is, thus, firmly linked to the *lex causae*: where it is not possible to conclude that the parties had made an express or implied choice as to the proper law, English courts abandon any reference to the intentions of the parties and seek to identify the law "with which the transaction has the closest and most real connection."[55] Such exercise is undertaken on objective grounds, taking into consideration all the facts and circumstances of the contract; and not merely its subject matter or the means of discharging the payment obligation. Similarly, localising a breach of a contract relating to a crypto asset for the purpose of Gateway 7, though likely to consider issues such as localising obligations in respect of crypto assets, is equally likely to weigh up a vast range of considerations and will not turn on any one factor, such as the *situs* of the crypto asset itself.

Accordingly, under English law, where parties have not made an express choice of law in their contract, the *situs* of the crypto asset – whether as the subject matter of the contract or as consideration – is highly unlikely to feature or be determinative of establishing jurisdiction or identifying the *lex causae* in a cross-border dispute arising in contract.

---

54 *Altimo Holdings and Investment Ltd v Krygyz Mobile Tel Ltd* [2011] UKPC 7, paras. 71, 81, and 88 (Lord Collins); *VTB Capital Plc v Nutritek International Corp* [2012] EWCA Civ 808, paras. 99–101 (Lloyd Jones LJ, delivering a joint judgment).

55 Hugh Beale (ed), *Chitty on Contracts* (33rd edn, London: Sweet & Maxwell 2018), para. 30-006 (fn 16 and text).

2.2.2.2 *The EU*

Localising a contract relating to crypto assets is more complex under the EU rules. Jurisdiction under Article 7(1) of the Brussels I Recast Regulation is firmly framed in terms of location determined by reference to the *subject matter* of the contract:

> 7. A person domiciled in a Member State may be sued in another Member State:
>
> (1)(a) in matters relating to a contract, in the courts for the place of performance of the obligation in question;
> (b) for the purpose of this provision and unless otherwise agreed, the place of performance of the obligation in question shall be:
> – in the case of the sale of goods, the place in a Member State where, under the contract, the goods were delivered or should have been delivered,
> – in the case of the provision of services, the place in a Member State where, under the contract, the services were provided or should have been provided;
> (c) if point (b) does not apply then point (a) applies.

Hence, questions as to definitions and the scope of the Regulation: where a crypto asset forms the subject matter of a contract, is such contract one for the 'sale of goods' or 'provision of services' within the meaning of subparagraph (1)(b)? If so, where is the place of delivery of such goods, or the place of performance of such services? On the other hand, if subparagraph (1)(b) is inapplicable, what is the 'obligation in question' and where is its 'place of performance' for the purpose of subparagraph 1(a) which would, by virtue of subparagraph (1)(c), apply in the case?

The position is somewhat easier in respect of the *lex causae*, as Article 4(1) of Rome I is, by contrast, framed in terms of localising the relevant *party* to the contract:

> 1. To the extent that the law applicable to the contract has not been chosen [...], the law governing the contract shall be determined as follows:
>
> (a) a contract for the sale of goods shall be governed by the law of the country where the seller has his habitual residence;
>
> (b) a contract for the provision of services shall be governed by the law of the country where the service provider has his habitual residence.

The issues, thus, raised under Article 4(1)(a) and (b) Rome I are limited to those of definition identified in respect of Article 7(1) Brussels I Recast.

Accordingly, the *situs* of a crypto asset is unlikely to feature directly where the rules of EU PIL on contracts in which the parties have not made an express choice of governing law nor of forum are engaged. Nevertheless, the applicable rules in these circumstances may indirectly engage the issue, by localising such contracts by reference to acts and obligations in respect of crypto assets. Hence, clarification – whether by the CJEU or legislative amendments – would be desirable as to: (i) whether crypto assets are 'goods' and any provision of crypto assets a 'service,' for the purpose of these Regulations; and if so, (ii) where, in the absence of any contractual provision, a crypto asset is 'delivered' or 'provided' in a contract for the sale of goods or provision of services; and if not, (iii) what constitutes the 'obligation in question' and the place of performance in a contract relating to a crypto asset.

2.2.3 Consumer Contracts under EU Law

Finally, it is worth reiterating that, in practice, most end-users of crypto assets typically access the crypto sector through intermediaries, such as crypto asset exchanges and wallet providers. Such intermediaries will, more often than not, be professionals within the meaning of the Brussels I Recast and Rome I Regulations. Where, therefore, the end-users are consumers within the meaning of those Regulations, it is highly likely that the consumer contract provisions will apply. As with Article 4(1) Rome I, the relevant provisions under both Rome I (Article 6) and Brussels I Recast (Article 18) are framed in terms of the place where the relevant *party* (usually the consumer) has his habitual residence or domicile. Accordingly, the *situs* of the crypto asset, is unlikely to feature when a court determines jurisdiction and/or the *lex causae* in respect of consumer contracts.

2.3 *Fetch.AI Ltd v Persons Unknown: Tort*

In this application before the English courts, the Applicants alleged, *inter alia*, that Persons Unknown had obtained unauthorised access to the First Applicant's accounts with the Binance Exchange and effected a series of transactions at an undervalue, thereby causing the First Applicant loss in the excess of USD 2.6 million. By the present application, the Applicants sought against the 1st-3rd Respondent Persons Unknown: (i) a proprietary order designed to freeze either the assets which were removed from the First Applicant's account and/or to restrain third parties in possession of their traceable proceeds from dealing with them as though they were their own; and (ii) a worldwide freezing order against those who were knowingly involved in the fraud for the purposes

of freezing their assets worldwide. Given that it was uncertain whether the Persons Unknown were within the territorial jurisdiction of the England, the Applicants further sought (iii) permission to serve proceedings out of the jurisdiction.

Applying the three-limb test, HHJ Pelling QC, as a Judge of the High Court, considered there were good arguable cases for the proposed claims in, *inter alia*: (i) breach of confidence or misuse of private information where detriment was suffered, or will be suffered, within the jurisdiction, or results from an act committed, or likely to be committed, within the jurisdiction (Gateway 21); and (ii) restitution where…the enrichment is obtained within the jurisdiction, or the claim is governed by the law of England and Wales (Gateway 16).

The basis for the findings in respect of the claim for breach of confidence is noteworthy for several reasons. First, HHJ Pelling QC considered it necessary to consider the private key supplied by Binance to the First Claimant for the purpose of operating its account, and found that:

> The private key is some code that is needed in order to operate the account. It is perfectly clear that the key was confidential information because it was supplied to the applicant for the purpose of enabling the applicant to operate its own account. I am satisfied [… that] those who were actually involved in prosecuting the fraud obtained access to confidential information and manipulated the accounts belonging to the company in breach of the duty of confidence which necessarily attached in the circumstances.[56]

As argued elsewhere, the facts of the case, on a closer analysis, do not disclose a cause of action sustainable in law.[57] The basic concepts underpinning the action of breach of confidence may well be apposite for the private key in empirical terms: a fragment of code that has a one-time value in proposing a transfer of crypto assets to the relevant decentralised ledger network, and which, therefore, must be kept confidential. Nevertheless, given the formal elements of the action, a claim for breach of confidence cannot be said to have been arguable in the present case;[58] nor can breach of confidence

56 *Fetch.AI* (n 26), para. 10.

57 Amy Held and Matthias Lehmann, "Hacked Crypto-Accounts, the English Tort of Breach of Confidence, and Localising Financial Loss under Rome II" (2021) 10 Journal of International Banking and Financial Law 708.

58 As set out in *id.*, 710: "The three-limb test for breach of confidence was set out in *Coco v AN Clark (Engineers) Ltd* [1968] FSR 415: (i) the information itself must have the necessary quality of confidence; (ii) the information must have been imparted in circumstances

adequately provide a means to vindicating interests in private keys as a general proposition.

The case, however, remains nevertheless interesting in the present context, as an illustration of how claims involving crypto assets, even those asserting a proprietary interest, may be characterised and vindicated via tortious causes of action. In respect of the proposed claim in breach of confidence, HHJ Pelling QC considered that this English cause of action was a 'tort/delict' for the purpose of Article 4(1) of the Rome II Regulation, which states:

> Unless otherwise provided for in this Regulation, the law applicable to a non-contractual obligation arising out of a tort/delict shall be the law of the country in which the damage occurs irrespective of the country in which the event giving rise to the damage occurred and irrespective of the country or countries in which the indirect consequences of that event occur.

Hence, the material question was identifying "the law of the country in which the damage occurs." Notwithstanding that localising damage in cases of pure economic loss, independent of personal injury or physical damage, raises difficult questions, these have been considered extensively by both the English and EU courts. Hence, the editors of the present edition of *Dicey, Morris, and Collins* state, at least for the purposes of the Rome II Regulation:

> ...if the defendant has induced the claimant to enter into an unfavourable transaction with a third party, it may be that the claimant should be taken to have suffered damage at the point, and in the place, where the claimant or his or her representative takes the steps necessary on his part to commit to the transaction. If, however, the induced transaction is with the defendant, it may be that the place from where the claimant

---

importing an obligation of confidence; and (iii) there must be an unauthorised use of that information to the detriment of the rights holder. Although the private key, prima facie, has the necessary quality of confidence (limb 1), and there is no dispute that there was unauthorised use of that information to the detriment of the Applicants (limb 3), limb 2 was problematic for the Applicants. It cannot be said that the Applicants imparted the confidential information to the Persons Unknown in circumstances importing an obligation of confidence; if anything, it was *Binance* who, having imparted the confidential information to the Applicants, might plausibly bring an action for breach of confidence. In that case, the proper defendant would be the Applicant, not the Persons Unknown. This, however, removes the cause of action far from the facts of the present case." It is, accordingly, submitted that the decision was wrong in law.

> or his or her representative takes the steps necessary to perform his or her obligations towards the defendant (e.g. by transferring funds from a bank account held at a particular branch) is to be preferred, on the basis that no irreversible loss is suffered until the claimant commits himself to performance. In misappropriation cases, it seems appropriate to locate damage at the place where an asset (tangible or intangible) is taken from the claimant's control.

Similarly, there is a long-standing line of case law of the CJEU – notably *Kronhofer*,[59] *Kolassa*,[60] and *Löber*[61] – on localising of damage under the Brussels I Recast Regulation and its predecessors, which, pursuant to Recital 7 of the Rome II Regulation, is to be followed when the latter Regulation applies.[62]

Accordingly, there is little need to consider the *situs* of a crypto asset where the real issues of the case arise in tort/delict.

2.4 *Ion Science v Persons Unknown: Trusts and Property*

Ion Science Ltd[63] has attracted considerable attention as the first case in which an English court considered the question of where a bitcoin is situate. The question arose in the context of an alleged ICO fraud in which the Claimants, an English company and its English-domiciled sole director and shareholder, alleged that they had been fraudulently induced by Persons Unknown – acting

59 Judgment of the Court (Second Chamber) of 10 June 2004, *Rudolf Kronhofer v Marianne Maier and Others*, [2004] ECR I-06009, Case C-168/02.

60 Judgment of the Court (Fourth Chamber) of 28 January 2015, *Harald Kolassa v Barclays Bank plc*, [2015], Case C-375/13 (ECLI:EU:C:2015:37).

61 Judgment of the Court (First Chamber) of 12 September 2018, *Helga Löber v Barclays Bank PLC*, [2018], Case C-304/17 (ECLI:EU:C:2018:701).

62 It is respectfully submitted, accordingly, that the Judge erred in law to localise damage in the case by reference to the allegedly confidential information. See further Held and Lehmann (n 57).

63 *Ion Science Ltd* (n 26). Having received confirmation from Mr Justice Butcher's clerk that the case was heard in private, the author has drawn upon the following commentaries: Syedur Rahman, "Ion Science Ltd v Persons Unknown" (*Rahman Ravelli*, 22 June 2021) <https://www.rahmanravelli.co.uk/articles/cryptocurrency-fraud-a-significant-judgement/> (who represented the Claimants); and Andrew Moir et al., "High Court considers where cryptocurrencies are located and compels disclosure of information by cryptocurrency exchanges outside the UK" (*Herbert Smith Freehills LLP*, 24 February 2021) <https://hsfnotes.com/litigation/2021/02/24/high-court-considers-where-cryptocurrencies-are-located-and-compels-disclosure-of-information-by-cryptocurrency-exchanges-outside-the-uk/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+HerbertSmithLitigationNotes+%28Herbert+Smith+Litigation+Notes%29#page=1>.

under the guise of a fictional Swiss financial entity – to effect a purported commission payment of approximately 64.36 bitcoin (GBP 577,002) in respect of a supposed cryptocurrency investment.

Accordingly, the Claimants brought proceedings in deceit, unlawful means conspiracy, and equitable proprietary claims in the bitcoin thus paid. By the present *ex parte* interim application, they sought, *inter alia*, a proprietary injunction, a worldwide freezing order, and an ancillary disclosure order against the Persons Unknown. To determine whether the Claimants should be permitted to serve out of the jurisdiction, Butcher J applied the three-limb test and made significant findings in respect of each stage of the test.

Butcher J considered that there were good arguable cases for claims: (i) in tort where damage was sustained, or will be sustained within the jurisdiction, or damage which has been or will be sustained results from an act committed within the jurisdiction (Gateway 9); and (ii) made against the defendant as a constructive trustee, or as a trustee of a resulting trust, where the claim arises out of acts committed or events occurring within the jurisdiction or relates to assets within the jurisdiction (Gateway 15).

Butcher J further found that there was at least a serious issue to be tried in respect of both (i) the merits of the claims; and (ii) English law as the applicable law governing the claims. Butcher J reached such conclusion on the *lex causae* on the basis that the damage occurred in England, given that, *inter alia*, England was the place where the bitcoin was situate prior to the fraudulent transfer. In reaching this conclusion on *situs*, Butcher J drew upon the proposal of Professor Dickinson that Bitcoin is situate where its owner is domiciled.

Finally, Butcher J considered England the appropriate forum because, *inter alia*, the Claimants were domiciled in England, the relevant funds were transferred from England, and, again, the bitcoin was situate in England prior to transfer.

Setting aside the merits or demerits of the proposition that bitcoins are situate where the owner is domiciled, it has been previously argued that the judge was wrong to find that there was a good arguable case under Gateway 15 in respect of the equitable proprietary claim: there is no clear authority for the proposition that a trust would arise on the facts of the case.[64] Rather, these are

64 Although there have been some obiter comments in the House of Lords that suggest a constructive trust is imposed in some circumstances where property has been obtained by fraud or theft, no clear authority has been cited to support such conclusions. The present editors of *Lewin* therefore conclude that "the position is still doubtful and it has not been clearly established that a thief is constituted as a constructive trustee. A first instance judge is probably bound by the view that no constructive trust arises." Thomas

almost on all fours with *Cundy v Lindsay,*[65] a classic textbook case on contractual mistake involving fraud perpetrated by an unknown rogue purporting to be a well-known firm.

Reliance on Gateway 15, therefore, was arguably misconceived; the 'true issues' of *Ion* arose in tort (and potentially contract) alone, rendering any discussion of where the assets were situate unnecessary. There is insufficient detail on the facts of the case to consider the Gateways relating to claims in contract; however, the Gateway under the tort claims could, in any event, have been established without reference to the *situs* of the relevant bitcoin. Rather, as with *Fetch.AI*, the exercise in localisation would have focused upon where the Claimants suffered loss, and by reference to other, more appropriate connecting factors, such as the place where the Claimants took the necessary steps to perform their obligations.

Notwithstanding, therefore, that the Applicants sought proprietary relief in respect of bitcoins, on a proper analysis in line with *Macmillan*, *situs* was irrelevant to the 'true issues' to be determined by the court. Had the issue been fully argued with the benefit of submissions made in opposition and to a higher threshold for the grant of relief, it is likely that the inapposite trust characterisation would have been challenged and the 'true issues' identified, as was the case in *Macmillan*, by the Defence. The case is, therefore, of less significance than has been assumed insofar as it concerns the *situs* of a bitcoin; and it has been previously argued[66] that more attention should be paid to the Judge's statement that his judgment should not be taken as authority for the proposition that bitcoins are situate in the place where its owner is domiciled.

Nevertheless, the case serves as a useful reminder that, even where a claimant asserts and relies upon an outright proprietary claim *in rem*, the *situs* of a crypto asset will be equally irrelevant should the claim be unarguable in law, or where the claimant's assertions are not actually part of the issues in dispute that, following *Macmillan*, form the subject of the exercise in characterisation.[67]

Lewin et al., *Lewin on Trusts,* Thomas Fletcher, Aidan Briggs, and Simon Adamyk (eds) (20th edn, London: Sweet & Maxwell 2020), para. 8-029.

65 *Cundy v Lindsay* (1878) 3 App. Cas. 459 (HL).

66 Held (n 29).

67 This is particularly important to recognise in the context of English equity, given the trend of claimants invoking equitable 'verbal formulae' in pursuit, usually, of more advantageous, proprietary remedies. Such trend has been the subject of stern rebuke from the Bench and in extra-judicial writings; see, for example, *Mothew v Bristol and West Building Society* [1993] AC 205, 16 (Lord Millett); Peter Millett, "Equity's Place in the Law of Commerce" (1998) 114 Law Quarterly Review 214, 217.

2.5 *Conclusions*

This section has demonstrated the extent to which concerns that PIL faces an 'intractable' problem in localising a crypto asset, fail to appreciate the significance of the characterisation exercise undertaken by the courts at the outset of any dispute. By reference to the decided cases, it showed that, notwithstanding that a cross-border dispute may concern a crypto asset, or that the pleadings may even assert proprietary claims to crypto assets, the true issues thrown up by the claim and defence may often be contractual or tortious in nature. It also drew attention to the fact that, given the highly intermediated nature of the contemporary crypto asset market, parties often transact on the basis of formal written contracts; accordingly, the characterisation exercise will often proceed on the familiar and largely unproblematic rules applicable to contracts. In sum, therefore, the *situs* of a crypto asset, in a significant number of cross-border disputes, will not, actually, matter.

3 When Situs Will, Actually, Matter

Notwithstanding the extent to which the relevance of *situs* may be undermined by characterisation, in some contexts, the facts of the case may raise a purely proprietary issue whilst the surrounding facts disclose no scope for an alternative characterisation in the law of obligations. The paradigm case is where the defendant and claimant have had no prior dealings with each other in law or fact, and the only thing that connects them is the fact the defendant has something that the claimant asserts belongs to him. Under English law, such purely proprietary claims are likely to arise in cases involving crypto assets allegedly misappropriated in breach of trust and/or fiduciary duty, or transferred by mistake; and the claimant, having traced and followed the assets now in the hands of a third party, seeks recovery of the asset from that third party through equitable proprietary claims or restitution. Under the present systems of PIL, the issues in such proprietary claims will unavoidably fall to be determined by those rules that refer to *situs*.

3.1 *The Outright Proprietary Claim*

To illustrate, consider the basic facts of *Macmillan*, slightly altered and borrowing from the User Agreements of Coinbase and Gemini. Suppose, then, that a New York-domiciled Claimant alleges that crypto assets held directly have been misappropriated in breach of trust by a trustee based in New York. The relevant assets having subsequently changed hands several times, our Claimant then follows and traces those crypto assets to public addresses attributable to (i) an Austrian domiciliary holding directly; (ii) a crypto Exchange incorporated and

registered in the Republic of Ireland; and (iii) a French domiciliary holding through the Exchange in a segregated Custody Account.[68] Upon disclosure, it transpires that: (iv) the Austrian domiciliary keeps her private keys on both a web wallet hosted by a server physically located in London, and as files saved to the local hard drive of her laptop physically located Vienna.

Under the terms of our Exchange's User Agreement, our French domiciliary has been informed and agrees with our Exchange that:

> By entering into a Custody Agreement,[69] you agree that you intend to create a bailment of Digital Assets with us, and you agree that you intend that we be the bailee.[70]
>
> Your Custody Account will have one or more associated unique Blockchain Addresses in which your Assets will be (i) segregated from any and all other assets held by us and (ii) directly verifiable via the applicable blockchain. We will provide you with all Blockchain Addresses associated with your Custody Account.
>
> The ownership of your Assets will be clearly recorded in our books as belonging to you. Our records will at all times provide for the separate identification of your Assets. We will not loan, hypothecate, pledge, or otherwise encumber any Assets in your Custody Account, absent General Instructions from you.
>
> You agree and understand that nothing herein prevents us from using our Cold Storage System to custody our own property and/or the property of third parties; provided, however, that, at minimum, separate Blockchain Addresses are utilized to segregate your Assets from such other property.[71]

Use of the term 'separate blockchain addresses' strongly suggests use of an HD seeded wallet to generate different public addresses for Custody Account clients.[72] For present purposes, the key feature to note is that such seed allows sequences of public keys to be generated, creating 'receive only' public

68 Gemini, "Custody Agreement" (*Gemini*, 7 April 2022), <https://gemini.com/custody-agreement/>.

69 *Id.*

70 *Id.*, "Custodian Appointment."

71 *Id.*, "Custody Account" (emphases added).

72 HD seeded wallets are hierarchical in that a single, cryptographically random "seed" is used to generate a master key, which in turn can be used to generate infinite generations of "children" and "grandchildren" keys. See more generally: Andreas Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchain,* (2nd edn, Sebastol: O'Reilly Media 2017), 96.

addresses, which function without requiring access to the private key.[73] As such, and under the terms of the User Agreement, our French domiciliary purportedly holds legal title to the crypto assets attributable to his public address, but does not hold the means to controlling these assets, *i.e.*, the private key. These are held by our Exchange, to whom the relevant crypto assets are purportedly bailed.

Finally, Clause 13 of the User Agreement provides for governing law and jurisdiction in the following terms:

> 13. This Agreement and the relationship between us shall be governed by the laws of Ireland and the non-exclusive jurisdiction of the Irish courts, subject to any local mandatory law, or rights available to Consumers.[74]

Accordingly, our Claimant has three potential Defendants, who are domiciled in France, Ireland, and Austria. In addition, our Claimant may seek to bring claims in England on the basis that our Austrian domicilliary's private keys – or one copy of them, at least – are stored on a server located in London. The immediate difficulty is, however, that the governing law and dispute resolution provisions in Clause 13 of the User Agreement will not be binding on our Claimant vis-à-vis any of her proposed Defendants, given that she is not herself party to the User Agreement. This, then, raises the 'intractable' questions: which court has jurisdiction; how is the claim to be characterised; and what law applies to the claim?

3.2 *England and Wales*

3.2.1 Jurisdiction

Given that there is no defendant within the territorial jurisdiction of England and the claim rather rests upon the server in London, our Claimant will need to identify a Gateway under CPR Practice Direction 6B paragraph 3.1 upon which to rely in an application for permission to serve our Austrian Defendant out of the jurisdiction. Our Claimant has several alternatives, which will be considered in turn.

---

73 Such arrangements are recognised as particularly effective for implementing organisational structures, such as allocating separate public addresses to different payees derived from a single master key.

74 Coinbase (n 48), Clause 13.21.

3.2.1.1 *Gateway 15: Claims about Trusts, etc.*

> 15. A claim is made against the defendant as constructive trustee, or as trustee of a resulting trust, where the claim arises out of acts committed or events occurring within the jurisdiction or relates to assets within the jurisdiction.

Gateway 15 is an attractive option for our Claimant. As her assets were misappropriated in breach of trust, her claim against our Austrian Defendant as a constructive trustee is sound in law. However, our Claimant must also establish that the claim arises out of acts committed or occurring within the jurisdiction, or relates to assets within the jurisdiction. Given that the breach of trust occurred in New York, she has no alternative but to submit that the relevant assets are within the jurisdiction. Although there is no direct authority as to the meaning of 'asset within the jurisdiction' for the purpose of Gateway 15,[75] the issue has been considered in the context of Gateway 11, another of our Claimant's alternatives, which is framed in materially the same terms.

3.2.1.2 *Gateway 11: Claims about Property within the Jurisdiction*

> 11. The subject matter of the claim relates wholly or principally to property within the jurisdiction, provided that nothing under this paragraph shall render justiciable the title to or the right to possession of immovable property outside England and Wales.

As a starting point, in *Re Banco Nacional de Cuba,*[76] Lightman J held that what is now Gateway 11 is: (i) not limited to land, but encompasses personal property, including intangibles such as shares in a company; nor (ii) limited to claims to a proprietary or possessory interest, rather, it suffices that the whole claim 'relates to' property.[77]

Hence, the more recent case of *Vidal-Hall v Google Inc*[78] considered the question of whether confidential information – in that case, browser generated

75 The Commentary focuses rather on the meaning of a trust. See "Notes on Heads of Jurisdiction in Paragraph 3.1 of Practice Direction 6B" in Peter Coulson et al. (eds), *Civil Procedure, Volume 1* (London: Sweet & Maxwell 2021), Part 6, para. 6HJ.30 ("White Book").

76 *In Re Banco Nacional de Cuba* [2001] 1 WLR 2039.

77 *Id*., para. 33 (Lightman J).

78 *Vidal-Hall v Google Inc* [2014] EWHC 13 (QB).

information – is 'property' for the purpose of Gateway 11. Described by Tugendhat J as a "question of law of some difficulty," Tugendhat J continued that the issue may not arise for consideration at trial, and if it were to be raised on an interim application, it should be in "circumstances where the parties have had a proper opportunity to put the relevant evidence and submissions of law before the court."[79]

On the other hand, *Ashton Investments v OJSC Russian Aluminium*[80] concerned a claim asserting breach of confidence in circumstances where the Claimant alleged that the Russian Defendants had hacked the Claimant's computer systems, which were maintained from servers physically located in London. To found jurisdiction, the Claimants sought to rely on, *inter alia*, what is now Gateway 11 on the basis that "the claim for breach of confidence related to property located within the jurisdiction." Citing *Re Banco Nacional de Cuba,* the Claimants submitted that 'property' for the purpose of Gateway 11 extended to personal property, intellectual property, and confidential information; the Claimant's computer system and the confidential information contained thereon fell, therefore, within its scope.[81] It should be noted, however, that such submission, insofar as it related to confidential information, was not challenged before the court.

On this unchallenged basis, Jonathan Hirst QC, as a Deputy Judge of the High Court, began from the premise that, as the relevant server was located in London, this was also where the relevant confidential and privileged information was situate.[82] Having then noted that the scholarship suggested that intellectual property fell within the definition of 'property,' the Deputy Judge concluded that Gateway 11 extended to claims in respect of confidential information "if it can be established that the information was really located in the jurisdiction. Information contained in digital form on a server in London satisfies this test."[83]

It is worth pausing here to consider the grounds upon which our Claimant may assert any claim to the server. On a technical analysis, the server is relevant to the dispute only insofar as it hosts a copy of our Austrian Defendant's private key. Private keys are the sole means through which a user may propose a change in state to the relevant decentralised ledger network; as such, according to one view, private keys are considered equivalent to the crypto asset itself. On the

79 *Id*., para. 140 (Tugendhat J).
80 *Ashton Investments v OJSC Russian Aluminium* [2006] EWHC 2545 (Comm).
81 *Id*., paras. 66–67.
82 *Id*., para. 62.
83 *Id*., para. 68.

author's own legal property analysis,[84] it is, however, important to distinguish the private key and the crypto asset as two distinct things; both of which may be the subject of proprietary and/or possessory claims. Consider, for example, the way in which our French domiciliary's Custody Account with our Exchange operates: the parties intend (i) that our French domiciliary holds title to the crypto asset; (ii) which is bailed to the Exchange; in (iii) factual circumstances where the private key associated with our French domiciliary's public address is held by our Exchange. There are, accordingly, at least two valuable interests associated with crypto assets under a purported bailment – essentially, that of title/ownership and that of immediate control/possession – which, not only vest in two separate persons, but also raise different considerations for the purpose of formulating a claim under the established causes of action.

How such empirical analyses translate into legal terms cannot be underestimated: there is a significant difference, for example, between an injunction to restrain our Exchange's use of a private key stored on a server as the means to controlling a separate asset, *i.e.*, the crypto assets[85] 'owned' by one of its Users; and an outright proprietary claim to the server itself – including the data comprising the private key stored thereon – as the physical 'embodiment' of the crypto asset analysed as the private key. Further issues arise as to the correct parties to the dispute: where, in the case of the Exchange Custody Agreement, our French domiciliary purportedly holds title to the crypto asset and the Exchange holds the private key as bailee, much will depend on whether the claim is made to the private key as the functional equivalent to the interest of possession (in which case, the claim should proceed against our Exchange, as bailee), or the private key as the effective equivalent of the crypto asset itself (in which case, the proper defendant would be our French domiciliary, as 'owner').

Irrespective of the exact legal property analysis, it suffices for the present purposes of our Claimant's case before the English courts that a parallel may be drawn between, on the one hand, the browser generated information and confidential information stored on the server in *Ashton Investments*, and, on the other, the copy of our Austrian domiciliary's private keys – analysed as pure data – held in a web wallet stored on our server in London. Applying, then, these precedents to our case, there is some authority to support the propositions that: (i) private keys are situate on the physical chattel on which they

84 Held (n 35), "Intermediated Cryptos: What Your Crypto Wallet Really Holds."

85 Under English law, such injunctive relief is not *in rem* but *in personam* against the respondent personally; accordingly, the application, at least, would not relate to property in the jurisdiction.

are recorded and stored; and (ii) presence of that physical chattel within the jurisdiction suffices to establish jurisdiction under Gateways 11 and 15.

The key issue for our Claimant, however, is that our Austrian domiciliary keeps multiple copies of her private key: one in London, one in Vienna. On any property analysis of private keys, there is no reason why the copy in London should be preferred over the copy in Vienna for the purpose of cross-border proceedings. Accordingly, the proposition that a private key – or, indeed, any pure intangible that exists in digital form – is situate where the chattel upon which it is recorded or stored does not solve the issue of localisation for the purpose of establishing jurisdiction in a cross-border dispute.[86]

Assuming, however, that in the absence of any other proposed fictional *situs* the analysis in *Ashton Investments* holds, a further consideration is that establishing that a Gateway applies is one of only three requirements for the test to serve out of the jurisdiction. Given that our Claimant must also satisfy the court that England is the convenient forum, it is highly likely that any application relying on Gateways 11 and 15 would likely fail on *forum conveniens* grounds: if an equally valid copy of the private key is situate, using the same technique of localisation, in the same jurisdiction as the intended Defendant, it is likely that the English courts would decline jurisdiction and/or stay proceedings in favour of the Austrian courts.

Accordingly, it is worth noting that, even if the situation of a crypto asset is relevant for the purposes of an application to serve proceedings out of the jurisdiction, it will not be decisive for the outcomes of any such application. Considerations such as *forum conveniens*, the proper exercise of jurisdiction, as well as the existence of a serious issue to be tried, may well outweigh the question of establishing a Gateway, rendering the localisation of the crypto asset purely academic.

3.2.2 Lex Causae

The English choice-of-law provisions for immovables and tangible movables are both reasonably clear: the general rule, subject to a few exceptions in the case of tangible movables, is that issues as to rights of property are determined by the *lex situs*.[87]

---

86 See *supra* Part I.

87 This was commented on in *Macmillan* (n 12), 399F-H. Staughton LJ cited *Norton v Florence Land and Public Works Co* (1877) 7 ChD 332 in respect of land and *Cammell v Sewell* (1860) 5 H & N 728, 744–745 in respect of chattels. With respect to the latter case, Staughton LJ further noted that: "Crompton J quoted Pollock CB in the court below (1858) 3 H & N 617, 638: 'If personal property is disposed of in a manner binding according to the law of the country where it is, that disposition is binding everywhere.' This was treated as the

The choice-of-law rules that govern transfers of intangible property, however, have been described as "not easy to state with certainty." The principal reason for this, in the view of the present editors of *Dicey, Morris, and Collins*, is worth restating here in full:

> ...the category of intangible things covers a very wide spectrum of property and rights, ranging from simple contractual debts, to shares in companies, to the securities and other financial instruments whose issue and trading underpins much of the capital markets of the developed world. All these may be seen as intangible property which is substantially contractual in origin. But other intangibles, such as a right to sue a tortfeasor, rights arising under trusts, rights in intellectual property, etc., do not have an obviously contractual origin. It is unrealistic for a single choice of law rule to govern all issues relating to the assignment of all such property. The basic choice of law rule of the common law for the assignment of intangible property was arguably intended to deal with the transfer or assignment of simple contractual intangibles such as debts, as distinct from more complex rights [...] for those intangibles which are not contractual in nature, a choice of law rule designed for the assignment of contractual rights will have no immediate justification for application. Consequently the choice of law rules for the assignment of intangible property have to cover an unusually wide range of legal situations, with the result that caution is required when stating and applying a rule to a factual context to which it has not previously been held to extend, or in applying a rule which is contractual in nature to a context which is not. It may even be argued that the category of "intangible things", the choice of law rules for the assignment of which were developed and refined by Dr Morris in order to state the common law rules of the conflict of laws, is no longer sufficiently coherent for it to be given a uniform rule for choice of law...[88]

Nevertheless, the editors consider that, although the proposition that there is a single choice-of-law rule that applies to all assignments of intangible things "cannot be completely correct," the basic approach of the common law appears

---

general rule, although subject to exceptions, in *Winkworth v Christie Manson and Woods Ltd* [1980] Ch. 496. It was applied by the House of Lords to a dispute about priority in *Inglis v Robertson* [1898] AC 616."

88 *Dicey, Morris, and Collins* (n 3), para. 24-051.

to have been that there is a uniform choice-of-law rule for the assignment of intangible things. [89] Such rule is stated in Rule 135:

> (1) As a general rule,
>
> (a) the mutual obligations of assignor and assignee under a voluntary assignment of a right against another person ("the debtor") are governed by the law which applies to the contract between the assignor and assignee; and
>
> (b) the law governing the right to which the assignment relates determines its assignability, the relationship between the assignee and the debtor, the conditions under which the assignment can be invoked against the debtor and any question whether the debtor's obligations have been discharged.

The editors plainly recognise, however, that there are several conceptual difficulties posed by the rule, which ultimately derive from the fundamental issue of whether and to what extent assignments of *choses* in action should be seen as raising a proprietary question at all:

> In relation to the assignment of rights which arise under a contract, such as a simple contractual debt, assignment may be seen as an aspect of the purely contractual question of who is presently entitled, as against the debtor, to enforce the right to payment. Such cases may belong, for the purposes of the conflict of laws, within the rubric of contract [...] but if this same issue is formulated as one which asks who owns the debt (that is, was the assignment of it effective to transfer it), the issue may present itself as proprietary in character. In relation to the voluntary assignment of intangibles other than contractual debts, such as shares in a company, or intellectual property rights, the right assigned is much less clearly contractual in origin, but the right is itself created and defined by a particular law in a manner analogous to contractual rights, and questions of assignment could also be seen as an incident of the law which created the right.[90]

89 *Id.*, para. 24-052.
90 *Id.*

These considerations came to the fore in *Raiffeisen Zentrallbank v Five Star Trading LLC*,[91] which involved an insurance policy taken out by certain shipowners in respect of a vessel, the *Mount I*, with French insurers. The shipowners then assigned the benefit of the policy to the Claimant Financer ("Raiffeisen") under a Deed governed by English law. When the *Mount I* collided with another vessel, thereby causing the other vessel to sink, proceedings were brought by the owners of the cargo that had been on board the sunken vessel, who ultimately obtained a French attachment order over the proceeds of the insurance policy. Raiffeisen accordingly sought a declaration that, *inter alia*, it was the person entitled to the proceeds of the insurance policy.

Mance LJ, with whom the other members of the Court agreed, considered that, notwithstanding that debts and other bilateral claims against an obligor are often subject to proprietary claims, in the ultimate analysis, the question of who 'owns' a debt will (correctly, it is submitted) centre on who is entitled to sue:

> The dominant theme influencing the modern international view of contract is party autonomy. Parties are … free to cancel or novate their contracts and make new contracts with third parties. A simple issue whether a contractual claim exists or has arisen in these situations cannot be regarded as an issue about property, however much an acknowledged contractual right may be identified as property in certain other contexts. An issue whether a contract has been novated appears to me essentially contractual …
>
> The cargo owners seek to redescribe the issue as being whether the title to the right of suit or cause of action which formerly vested in the assignor was vested in or was now owned by the assignee. In this way they seek to give the issue a proprietary aspect. However, it is unclear why it is necessary to talk of "title to the right", or to focus on its transfer from assignor to assignee, rather than upon the simple question: who was in the circumstances entitled to claim as against the debtor? The artificiality seems to me to be underlined at the next stage of the argument, which seeks to refer any dispute about title to sue to the place where the "property" consisting of such title is "situated."[92]

91 *Raiffeisen Zentrallbank v Five Star Trading LLC* [2001] EWCA Civ 68.
92 *Id.*, para. 34 (Mance LJ).

Hence, the primary difficulty in applying Rule 135 to crypto assets: properly analysed, they are in no way a '*chose* in action' proper, *i.e.*, underpinned by a claim against another person, whether contractual, tortious, or, in the words of *Dicey, Morris, and Collins*, "in a manner analogous" to a contractual right. There is no, in the words of Mance LJ, debtor against whom the question of entitlement to sue is raised. Nor is there, for the purpose of Rule 135 (1)(b), "law governing the right to which the assignment relates," *i.e.*, a *lex creationis* to which to refer for the purpose of ascertaining the governing law.

On the author's own analysis of the facts underpinning an unpermissioned ledger, the most that can be said[93] is that the value of a crypto asset is grounded in the right to be recognised as participating in a decentralised ledger network with a defined quantum of value – as recorded in the decentralised ledger and attributable to a public address – by other participants in that network. Any potential claim would, accordingly, be brought most appropriately against the other participants of the network as a collective for an alleged breach of an implicit agreement between them as to how the network is to operate. As such, there are many parallels in fact that may be drawn with shares in companies or participation in an unincorporated association, however, crypto assets must be distinguished on the basis that there is not yet any enacted *lex creationis* – akin to the Companies Act 2006 and its predecessors for shares generally, or implied contract for unincorporated associations – that 'creates and defines' the corresponding right or valuable asset "in a manner analogous to contractual rights." Similarly, although a private key has much in common with intellectual property rights, in the absence of any *lex creationis* akin to the Copyright, Designs, and Patents Act 1988 or Patents Act 1977, there is no underlying law that can be held to govern questions of priority where multiple claims are made to a private key. Again, if an alternative analysis emphasising the decentralised ledger is favoured, crypto assets cannot be considered registered assets in the absence of any statutory or other *lex creationis* – comparable to the CREST Regulations[94] for uncertificated securities – pursuant to which the decentralised ledger is given legal recognition as a definitive title register.

The conceptual difficulty is somewhat obscured by the historical development of the English property taxonomy and terminology, rather than the choice of law rules *per se*. For many centuries, the contract debt comprised the most economically significant type of intangible asset; equal to, if not

93 See further, Held (n 25), " Private Keys v Blockchains: What is a Cryptoasset in Law?."

94 The Uncertificated Securities Regulations 2001, SI 2001/3755. See further the discussion below at 3.3.1.2 relating to "public registers" within the meaning of Art. 24(3) of the Brussels I Recast (n 50), especially (fn 102).

supplanting, land as traditional feudal socio-economics gave way to capitalism.[95] Accordingly, the assignable contract debt has shaped both the property taxonomy and terminology: '*chose* in action' is often taken as definitive and/or exhaustive of the category of intangible assets; 'assignment' generally tends to be used for transfers of intangible assets, as opposed to 'conveyance' or 'transfer'; proprietary interests in such assets as 'enforced', not 'vindicated.' Such terminology and taxonomy often obscures the fact recognised in *Dicey, Morris, and Collins* that intangible assets as a category comprise a wide range of assets, not all of which are contractual in character. Applying a rule developed in the context of a contract debt to those which are inherently not contractual, it is submitted, can yield only unsatisfactory results. It cannot be coincidental that both shares in companies and intellectual property rights are recognised, not only as 'less obviously contractual in nature,' but also without the general rules for intangible assets in both the English and EU systems of PIL and, instead, are subject to their own, dedicated provisions.[96]

Hence, crypto assets are the prime example of a type of intangible asset to which Rule 135 cannot apply. The primary difficulty is, however, that there are presently no other rules for 'intangible property' that are not properly *choses* in action; as noted above, the academic authorities consider that that Rule 135 represents a 'uniform rule' governing the transfer of all intangible things. Accordingly, it is submitted that reform to both the English law of property and the rules of PIL applicable to intangible property is required to accommodate modern digital assets. One particular issue requiring attention is that *choses* in action, properly defined as based upon an obligation and corresponding claim to performance, are: (i) neither exhaustive of the category of intangible assets; nor (ii) capable of serving as a comparable model for intangibles, such as crypto assets, that are not based on the concept of an obligation and claim.

3.3 *The EU*

3.3.1 Jurisdiction

Under the rule of general jurisdiction of Article 4 of the Brussels I Recast Regulation, our Claimant must sue each of our Exchange, Austrian, and French

95 Although the link between capitalism and legal developments in the 18th and 19th century may not be immediately obvious, specialist legal scholarship convincingly demonstrates the full extent to which the modern law of contract developed to support and give legal effect to capitalist commercial practices centred on a new concept of wholly promissory liability. See, in particular, Patrick Selim Atiyah, *The Rise and Fall of the Freedom of Contract* (Oxford: Clarendon Press 1979).

96 See, for example, under Brussels I Recast (n 50): Art. 24(2) for companies; Art. 24(4) for intellectual property.

domiciliaries in, respectively, Ireland, Austria, and France. Alternatively, our Claimant may, under Article 8(1), opt to sue all three proposed EU Defendants in one of Ireland, Austria, or France, provided that the claims are so closely connected that it is expedient to hear and determine them together to avoid the risk of irreconcilable judgments.

Hence, the issue of characterising each of the claims our Claimant seeks to bring against each Defendant. Before, however, any consideration of whether these claims may justify joinder under Article 8(1), it is necessary first to ascertain whether any of the proposed claims fall within the provisions for exclusive jurisdiction.

3.3.1.1 *Rights in Rem in Immovable Property*

Article 24(1) provides:

> In proceedings which have as their object rights in rem in immovable property or tenancies of immovable property, [exclusive jurisdiction is conferred on] the courts of the Member State in which the property is situated.

This immediately raises a key question, again, relating to characterisation in property disputes: are crypto assets immovables within the meaning of Article 24(1)?

There is presently no express EU definition of the terms 'immovable' and 'movable' property. As such, national courts in attempting to apply what must nevertheless be an autonomous EU definition will realistically have recourse to principles shaped by their own national property laws. However, this raises a difficult question that is inherently circular. Issues of characterisation arising in a claim are usually determined according to the *lex fori*. However, as noted in Part 1, proprietary claims are unique insofar as the characterisation exercise is concerned: most, if not all, jurisdictions determine characterisation of things as either movable or immovable according to the *lex situs*.[97] The *situs* of a crypto asset is, thus, immediately brought into question which, in the case of a proprietary issue *in rem*, cannot be circumvented.

In principle, the issue could be overcome by adopting a fictional *situs*; there is no reason why only movables should benefit from judicial fictions ascribing to assets with no physical location, an artificial location to bring them within the scope of those rules of PIL expressed in terms of *situs*. If, therefore, the *lex*

97 See *supra* (n 2) and (n 3).

situs rule is to be maintained in respect of crypto assets as the subject of proprietary claims, the proposals set out in Part 1 above for ascribing an artificial situs to crypto assets warrant serious consideration.

In all cases, guidance as to whether crypto assets are movable or immovable property for the purposes of the Brussels I Recast Regulation would be desirable to ensure national courts do not have undue recourse to the substantive property law of the forum in applying what must be an autonomous EU definition.

3.3.1.2 *Validity of Entries in Public Registers*

A further exception from the general rule of jurisdiction potentially relevant for our Claimant relates to public registers. Article 24(3) states:

> in proceedings which have as their object "the validity of entries in public registers," [exclusive jurisdiction is conferred on] the courts of the Member State in which the register is kept.

Unlike Article 24(1), Article 24(3) has largely been unproblematic and has generated little case law. It should, however, be noted that the provision covers proceedings that put in issue the validity of entries in the register, rather than, for example, the consequences of entry into the register, or the conditions for entry.[98]

Article 24(3) is of particular interest for our Claimant, given that (i) the original function of the decentralised ledger is to generate an immutable and definitive public record of changes in state;[99] and (ii) many subsequent applications of DLT expressly designate the decentralised ledger as a definitive register of title in respect of (usually) off-chain assets that are, according to the intentions of the parties, registered assets.[100] Accordingly, the basic preliminary question is whether decentralised ledgers are 'public registers' within the meaning of

98 van Calster (n 10), para. 2.195.

99 See generally Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (*Bitcoin*, 31 October 2008), <http://nakamotoinstitute.org/Bitcoin/>.

100 Blockchain bonds, for example, have been issued over the Ethereum network as registered assets; settlement systems, such as the Australian Stock Exchange, have adopted DLT solutions for their internal records; the Deutsche Börse – HQLAx digital collateral solution operates on the basis of the registered model of assets within the intemediated system for dematerialised securities. See further Amy Held, "Crypto-Financial Assets in a DLT-Based Market Infrastructure: Legal Principles of Ownership and Obligation" (LL.M Masters Coursework Thesis, University of Melbourne 2019) <http://hdl.handle.net/11343/274809>.

Article 24(3). Only if this is so will the question of localisation, *i.e.*, where are such registers 'kept,' be necessary to address. Finally, in any given case, it will be necessary to establish that the proceedings bring in issue the validity of an entry in the register.

In respect of the first question, it is necessary to consider the definition of 'public.' Decentralised ledgers, as originally conceived of in the Bitcoin White-paper, are often referred to as 'public' in that they are freely available to all members of the public on an open-source licence. Anyone may, therefore, download the relevant source code and participate in a public decentralised ledger network designed to record transactions transparently announced and agreed upon by the network participants themselves. The critical point is that such consensus is achieved without recourse to a third-party trusted intermediary – typically a private institution – whose records are ultimately guaranteed by the State.

Such concept of 'public' must be distinguished from, and was indeed designed to challenge, the normative concept of 'public' in the sense of being endorsed by the State in an exercise of sovereign power. Article 24(3), however, arguably applies to 'public registers' in this latter sense: the examples set out in the *Jenard* Report of registers falling within the scope of Article 24(3) – land registers, land charges, and commercial registers[101] – share a common basis in some legislative act or other exercise of sovereign authority from which their 'public' (and legally definitive) nature derives. Thus, it has been argued, at least in the context of the UK, that decentralised ledgers "cannot operate as definitive title registers unless statute has given it binding legal effect; in the absence of such legislation, a court will not, if required to determine proprietary rights to a crypto asset, be bound by the position maintained in the ledger."[102] A court may well, however, consider such ledgers as definitive of ownership pursuant to contractual arrangements – express or implied – between the participants of the network *inter se*.

The issue is particularly well-illustrated when contextualised within the second substantive requirement of Article 24(3), namely, that the proceedings put in issue the validity of entries in a register. From a coding perspective, entries on the blockchain, having passed the rigorous tests of validity and consensus coded into the protocol, are designed to be immutable. For proponents of the 'code is law' position, there is no scope to challenge the validity of an entry

101 Jenard Report (n 7), 35.

102 UK Jurisdiction Taskforce, "Legal statement on cryptoassets and smart contracts" (*The LawTech Delivery Panel*, November 2019), para. 132 <https://technation.io/lawtech-uk-resources/#cryptoassets> accessed 30 June 2023.

on an unpermissioned decentralised ledger: entry and continued presence on the agreed version of the ledger is, in itself, proof of its validity. Only if, therefore, an unpermissioned decentralised ledger is placed on a legal basis will it be likely that legal claims will be brought in respect of the validity of its entries.

Accordingly, it is doubtful that a decentralised ledger, without more, will be considered a 'public register' within the meaning of Article 24(3).

3.3.1.3 *Conclusions on Jurisdiction*

For our Claimant, then, it does not appear that any of the provisions for exclusive jurisdiction will apply. It follows that she must rely on the general rule of jurisdiction and bring proceedings in Ireland, Austria, and France. Alternatively, if the respective claims against each Defendant are sufficiently connected so as to justify joinder under Article 8(1), she may bring proceedings in one of the three jurisdictions.

The difficulty, however, in determining whether the claims are 'sufficiently connected' at the jurisdiction stage of proceedings is that it is not yet clear what claims and under what *lex cause* are being considered for this purpose. As will be seen, the relevant rules under the EU framework are inherently circular, leaving considerable scope for fragmentation and forum shopping.

3.3.2 Lex Causae

The statement that "in private international law, there is a fundamental distinction between property, which has its own choice of law rules, and obligations, to which separate choice of law rules apply"[103] is of particular relevance in the context of the EU Regulations on choice of law: both the Rome I and Rome II Regulations exclude property matters from their scope. As the Giuliano-Lagarde Report makes clear in its Commentary on Article 1 ('Scope of the Convention') of the Rome I Regulation:

> First, since the Convention is concerned only with the law applicable to contractual obligations, property rights and intellectual property are not covered by these provisions. An article in the original preliminary draft had expressly so provided. However, the group considered that such a provision would be superfluous in the present text… [104]

103 Torremans et al. (eds) (n 38), 789.

104 "Report on the Convention on the law applicable to contractual obligations by Mario Giuliano, Professor, University of Milan, and Paul Lagarde, Professor, University of Paris I," [1980] OJ C 282/1, 10. In English law, sec. 3(3) of the Contracts (Applicable Law) Act 1990

Nevertheless, it is clear that some proprietary matters do fall within the Rome I Regulation. Article 14 provides:

1. The relationship between assignor and assignee under a voluntary assignment or contractual subrogation of a claim against another person (the debtor) shall be governed by the law that applies to the contract between the assignor and assignee under this Regulation.
2. The law governing the assigned or subrogated claim shall determine its assignability, the relationship between the assignee and the debtor, the conditions under which the assignment or subrogation can be invoked against the debtor and whether the debtor's obligations have been discharged.
3. The concept of assignment in this Article includes outright transfers of claims, transfers of claims by way of security and pledges or other security rights over claims."

Recital 38, furthermore, expressly provides that:

> In the context of voluntary assignment, the term 'relationship' should make it clear that Article 14(1) also applies to the property aspects of an assignment, as between assignor and assignee, in legal orders where such aspects are treated separately from the aspects under the law of obligations. However, the term 'relationship' should not be understood as relating to any relationship that may exist between assignor and assignee … The term should be strictly limited to the aspects which are directly relevant to the voluntary assignment or contractual subrogation in question.

The position under Rome I is, thus, substantively the same as the English Rule 135. The same issues identified in respect of Rule 135 accordingly apply with equal force: on any analysis, there is no "law governing the assigned or subrogated claim" for the purpose of Article 14(2) Rome I; nor is there any 'claim' that has been assigned or subrogated at all. In the absence of any other provision or guidance from the CJEU, it appears that the proprietary issues – both substantive and relating to PIL – arising in a voluntary transfer of crypto assets pursuant to a contract, if pleaded, will fall to be determined according to national laws.

Similarly, the Rome II Regulation is widely recognised as excluding property matters altogether, as these do not form part of the law of obligations.[105] Any

---

provides that the Report "may be considered in ascertaining the meaning or effect of any provision of that Convention."

105 Torremans et al. (eds) (n 38), 808.

proprietary issues arising from non-contractual causes of action will accordingly fall to be determined also according to national laws.

Hence, within the EU, identifying the *lex causae* will largely fall to the domestic choice-of-law rules of the Member States. This, however, is problematic, given that most jurisdictions tend to apply the *lex situs* to property claims *in rem* and, failing any plausible candidate law in this respect, are likely to apply the substantive property law of the forum. Given, however, the extent to which national property laws – even within the EU – differ from jurisdiction to jurisdiction, this leads to an inherently circular process of legal reasoning as any claim asserted will necessarily be premised on the application of the law of a particular jurisdiction.

To illustrate, our Claimant has identified our Exchange, Austrian, and French domiciliaries as the persons receiving at the relevant public addresses participating in the decentralised ledger network to which she has traced her crypto assets misappropriated in breach of trust. Our Claimant, accordingly, seeks to assert claims against each as constructive trustees. However, in the absence of any clear choice of law rule that identifies the relevant *lex causae*, the Irish, Austrian, and French courts are likely to apply the substantive property law of the forum to the claim.

Accordingly, a claim asserting a constructive trust is likely to be recognised by the Irish courts as against our Exchange, applying the substantive property law of the forum to the claim in the absence of any plausible alternative. By contrast, such claim will unlikely be recognised as against our Austrian and French domiciliaries, unless the Austrian and French courts are satisfied that both (i) some other law, rather than the substantive law of the forum, applies to the claim; and (ii) that other law recognises the trust institution.

It is, thus, unclear what claims our Claimant actually has against each of her proposed Defendants, let alone whether they are sufficiently connected so as to justify joinder under Article 8(1) of the Brussels I Recast Regulation. Our Claimant, thus, appears to have no alternative but to rely on the default rule, and bring proceedings against each of her proposed Defendants in the courts of the Member State where they are domiciled.

In respect of our French domiciliary, that our Exchange holds the private keys paired with the public address at which our French domiciliary receives crypto assets adds a further consideration. Even if our Claimant is not party to the contract of bailment between our French domiciliary and Exchange, as a matter of fact, our Exchange has practical control over the crypto assets held at our French domiciliary's public address. This may well justify joinder under Article 8(1) of the Brussels I Recast Regulation. In the alternative, our Claimant may seek to obtain an order restraining the Exchange from dealing

with the crypto assets attributable to our French domiciliary's public address, either issued directly by the Irish courts, or by recognition by the Irish courts of an equivalent French order.

3.4 *Conclusions*

This section has explored the extent to which the present rules of PIL, both at English common law and under the EU system, will unavoidably refer to the *situs* of a thing in cross-border proprietary claims. It has showed that, in these circumstances, it is unclear whether crypto assets fall within the scope of these rules; and furthermore, in some circumstances, these rules are, on their own terms, simply inapplicable to crypto assets as the subject of proprietary claims. Insofar as there remains no clarification on scope of these rules, nor consensus as to any fictional *situs* of a crypto asset, nor alternative rules, legislative reform or binding guidance will be required to establish property law PIL regimes fit for modern purpose.

4 A Broader Criticism of *Situs* as a Connecting Factor

Given that the rules relating to the *situs* of an asset originally developed in relation to land and tangible goods, it is perhaps unsurprising that application of these rules to intangible assets have been problematic. If, as noted in Part 1, the rationale of the rule is ultimately grounded in concepts of territorial sovereignty, it has long been recognised that the concept of *situs* is less justifiable for intangible assets. Where, however, such assets are both legally abstract concepts lacking an underlying *lex creationis* and, furthermore, decentralised as a matter of fact, Westphalian concepts of territorial sovereignty simply cannot apply: what nation state can lay claim to territorial sovereignty over assets that exist, quite literally, nowhere and everywhere at once? As has been recently noted by Professor Matthias Lehmann, the intrinsic problem with defining jurisdiction over crypto assets is *not* the absence of any valid "genuine link" between such assets and a nation state, but the abundance of genuine links to several states, each in equal measure. Hence, his proposal for a new concept of 'omniterritoriality,' defined as a response to "those phenomena that cannot be linked to a specific country because they have simultaneous and equally valid connections to jurisdictions all over the world."[106]

106 Matthias Lehmann, "Extraterritoriality in Financial Law" in Austin Parrish and Cedric Ryngaert (eds), *The Cambridge Handbook on Extraterritoriality* (Cambridge: CUP 2022 forthcoming; manuscript with the author).

There is, therefore, no compelling reason why *situs* should be maintained as the relevant connecting factor, especially when to do so entails applying legal fictions that have already been recognised as sometimes yielding "unfortunate results… because the rationale of the [*situs*] rule may no longer be served where it is applied in this way."[107] Furthermore, recourse to *situs* for modern omniterritorial assets does not seem justifiable, given that its application even to tangible property has been challenged for almost a century. As early as 1935, Professor Cheshire expressed the view that:

> …the proposition that [questions concerning the acquisition or transfer of ownership of tangible movables are generally to be decided by the law of the situs], although it has the support of Cammell v Sewell, an authority which has never been impugned, can scarcely be regarded as an adequate guide for the future. The law relating to tangible moveables has remained practically stationary for more than half a century, and it is clear that the difficulties which support this subject cannot be satisfactorily determined by a simple reference of the lex situs.[108]

Even in 1950, it was noted that "there is …no unanimity on the reason why the law of the *situs* should be decisive."[109] By 1964, the primacy of the rule was questioned, with the suggestion that the *situs* had attained a special place as connecting factor, not by merit, but by "history aided by frequent repetition of often superficial argument by textwriters and judges."[110]

---

107 *Dicey, Morris, and Collins* (n 3), para. 22-025.

108 Geoffrey Chevalier Cheshire, "Private International Law" (1935) 51 Law Quarterly Review 76, 84, cited in Janeen M Carruthers, *The Transfer of Property in the Conflict of Laws: Choice of Law Rules in Inter Vivos Transfers of Property* (Oxford: OUP 2005), 8.16.

109 Martin Wolff, *Private International Law* (2nd edn, Oxford: OUP 1950), 511, cited in Janeen M Carruthers, *The Transfer of Property in the Conflict of Laws: Choice of Law Rules in Inter Vivos Transfers of Property* (Oxford: OUP 2005), para. 8.01 (fn 2 and text).

110 Ian F Baxter, "Conflicts of Law and Property" (1964) 10 McGill Law Journal 1, 34, cited in Janeen M Carruthers, *The Transfer of Property in the Conflict of Laws: Choice of Law Rules in Inter Vivos Transfers of Property* (Oxford: OUP 2005), para. 8.01 (fn 3 and text). The most trenchant and colourful criticism of a single rule, comprised of a broad, general principle to determine all cases, since then was described as: " … surely the hoariest fallacy of legal thinking – that a rule must be followed blindly, even in cases where it produces harsh and inconvenient results, for the sake of certainty, simplicity, uniformity and symmetry of the law" is in Moffatt Hancock, "Conceptual Devices for Avoiding the Land Taboo in Conflict of Laws: The Disadvantages of Disingenuousness" (1967) 20 Stanford Law Review 1, 10, cited in Janeen M Carruthers, *The Transfer of Property in the Conflict of Laws: Choice of Law Rules in Inter Vivos Transfers of Property* (Oxford: OUP 2005), para. 8.16.

In a more modern review of the rules based on situs, in 2005, Janeen Carruthers noted that 70 years since the first criticisms of the rule, "the same connecting factor continues, tenaciously, to be the conflict lawyer's guide, despite opportunities having arisen for changes or modifications to be introduced."[111] Carruthers further considered that there was little scope to challenge such position, as there had been:

> … a 'mechanical reiteration' of the arguments which support the rule, leading to the apparently unanimous conclusion that no other connecting factor is appropriate to deal with questions concerning the transfer of property. Widespread belief in the inevitability of the situs rule, and time-honoured, wonted arguments in support of the rule have been endorsed by the courts, which have conceded only a very narrow margin for evading the situs monopoly.[112]

Such 'widespread belief in the inevitability of the *situs* rule' certainly persists today, with the immediate assumption that PIL faces an 'intractable' problem in assets that neither have a physical *situs* nor are amenable to a reasonably logical or intuitive artificial *situs*; and the immediate recourse, nevertheless, to proposals for such artificial *situs*, as set out in Part 1 above. Implicit in such assumption and proposals is the premise that *situs* is an absolute connecting factor in all cases involving proprietary issues. There is, however, little to justify such premise. To the contrary, there are several reasons why a more flexible approach is justified.

4.1 *The Rules of PIL Change Over Time*

It is accepted that there is a modern consensus that proprietary disputes in respect of tangible assets are governed by the *lex situs*. This rule has been described judicially as being "long established beyond dispute,"[113] however, such consensus is, on closer analysis, a relatively modern phenomenon. Proprietary claims to personal movables were originally held governed by the law of the owner's domicile; such things being considered an intrinsic part of personality, rather than of property.[114] In 1854, Story argued against the application of the *lex situs* in respect of movables, citing both (i) uncertainty surrounding the

111 Carruthers (n 15), para. 8.17.
112 *Id*., para. 8.16, citations omitted.
113 *Air Foyle Ltd v Center Capital Ltd* [2002] EWHC 2535 (Comm), para. 42 (Gross J).
114 d'Avout (n 2), 1428.

situation of the asset in transit between different places; and (ii) the impracticality of knowing the law of *inter vivos* transfers applicable in those places.[115]

The rule based on domicile persisted until the early 20th century, when other possibilities, such as *lex situs, lex contractus, lex loci acti*, increasingly gained traction. By the 1930, the courts were firmly moving towards the application of the *lex situs*, though not without criticism.[116] Such developments in establishing a successor to the rule based on domicile was noted more recently with interest in *Glencore International AG v Metro Trading International Inc:*

> ...in the 7th edition of his Private International Law published in 1965 Professor Cheshire noted that there was then no English authority preferring the lex situs over the proper law of the transfer when the dispute was limited to the two parties to the transfer. He suggested that in such a case the proper law of the transfer was to be preferred on the grounds of principle and convenience, but that view was not repeated in the 8th edition published in 1970 or in subsequent editions in which some prominence is given to the dictum of Diplock L.J. in Hardwick Game Farm. The current (13th) edition of Cheshire and North's Private International Law simply states that "the application of the law of the situs rule must prevail on practical grounds of business convenience.[117]

Similarly, in respect of the priorities between competing assignments of a *chose* in action, there is a general consensus today that the proper law of the contract creating the assigned debt applies.[118] This, however, was not always the case: in *Macmillan*, Staughton LJ recognised that, in the first edition of *Dicey* in 1896,[119]

---

115 Joseph Story, *Commentaries on the Conflict of Laws* (London: Maxwell, 1841), 552 cited in Janeen M Carruthers, *The Transfer of Property in the Conflict of Laws: Choice of Law Rules in Inter Vivos Transfers of Property* (Oxford: OUP 2005), para. 8.32.

116 As illustrated obiter in *Re Anziani, Herbert* (n 12): "I do not think that anyone can doubt that, with regard to the transfer of goods, the law applicable must be the law of the country where the moveable is situate. Business could not be carried on if that were not so." In response: consider Wolff (n 109), 516, "[i]t was possibly a slight exaggeration when Maugham J said obiter [that the law of the *situs* must apply]...But at least this dictum states the goal to which the development of the English law tends and which it has probably attained." Consider also Cheshire's more succinct criticism: "It is submitted with respect that there is much room for doubt," Cheshire (n 13), 559. Both cited in Carruthers (n 15), para. 8.34.

117 *Glencore International AG v Metro Trading International Inc* (*No.2*) [2000] EWHC 199 (Comm), para. 19 (Moore-Bick J).

118 Rule 135 *Dicey, Morris, and Collins* (n 3); Art. 14(1) of the Rome I Regulation (n 50).

119 As cited in *In re Maudslay, Sons & Field* [1900] 1 Ch 602, 610 (Cozens-Hardy J).

the relevant rule referred to the *lex situs* of the debt.[120] However, for various reasons stated in the then-current or recent editions of both *Cheshire and North's Private International Law* (12th ed, 1992) and *Dicey & Morris* (12th ed, 1993; and 11th ed, 1987), Staughton LJ recognised that "*situs* is now replaced by the law of the contract by which the debt was created."[121] Furthermore, Staughton LJ recognised that, although in some cases involving choses in action, other solutions had been adopted in light of the specific circumstances of the case,[122] both the *lex loci acti* and the proper law of the assignment had also by then been rejected for the purpose of a general rule.[123]

4.2 *The Rules of PIL Are Not Absolute*

This leads conveniently to the second argument: courts have recognised that the rules of PIL law are not to be applied rigidly. In *Raiffeisen*, it was not in dispute that identifying the appropriate law involved a three-stage process[124] to be undertaken in "a broad internationalist spirit in accordance with the principles of conflict of laws of the forum."[125] However, Mance LJ expressed the view that, although 'convenient' to identify such process, "the conflict of laws does not depend (like a game or even an election) upon the application of rigid rules, but upon a search for appropriate principles to meet particular situations."[126] Hence:

> ...the overall aim is to identify the most appropriate law to govern a particular issue. The classes or categories of issue which the law recognises at the first stage [of characterisation] are man-made, not natural. They have no inherent value, beyond their purpose in assisting to select the most appropriate law. A mechanistic application, without regard to the consequences, would conflict with the purpose for which they were conceived. They may require redefinition or modification, or new categories

120 "An assignment ... of a debt, giving a good title thereto according to the lex situs of the debt (in so far as by analogy a situs can be attributed to a debt), is valid." Rule 141 *Dicey on the Conflict of Laws*, (1st edn, London: Stevens & Sons Ltd and Sweet and Maxwell 1896) cited in *Macmillan* (n 12), 401F (Staughton LJ).

121 *Macmillan* (n 12), 401G (Staughton LJ).

122 *Id*., 401G-402D (Staughton LJ).

123 *Id*., 402C-E (Staughton LJ).

124 As set out at *Raiffeisen* (n 91), para. 26 (Mance LJ): (1) characterisation of the relevant issue; (2) selection of the rule of conflict of laws which lays down a connecting factor for that issue; and (3) identification of the system of law which is tied by that connecting factor to that issue.

125 *Id*.

126 *Id*., para. 29 (Mance LJ).

> may have to be recognised accompanied by new rules at stage 2 [that lay down a connecting factor for the relevant issue] if this is necessary to achieve the overall aim of identifying the most appropriate law…[127]

The flexible application of the rules of PIL to a search for the "most appropriate" law to meet particular situations is particularly pertinent in the present context, where modern advances in technology have rendered obsolete many of the traditional distinctions and premises upon which the current rules of PIL for property are based. Even in *Raiffeisen,* Mance LJ recognised that the traditional situation of a debt at the habitual residence of the debtor, on the basis that this is where the debt could be enforced, was increasingly under strain because of modern conditions: jurisdiction being founded on other bases apart from residence; obligations being enforced against assets, not persons, and which are often traded or held abroad; and the move towards single markets and the free circulation of judgments between States.[128]

Hence, today, where the traditional concepts of domicile, habitual residence, and sovereign territoriality are increasingly challenged by omniterritorial concepts, it is submitted that rigid adherence to an ancient rule of conflict of laws originally developed for land and tangible movables is neither prescribed by a rule of law; nor in accordance with principles explicated by Mance LJ in *Raiffeisen* in respect of a flexible approach in search of the most appropriate principles to meet particular situations, recognising new categories and new rules, if necessary, to achieve this aim.

4.3 *Other Possibilities: Is It Time* Situs *Was Unseated?*

Accordingly, it is submitted that any further attempts to shoehorn crypto assets, as inherently omniterritorial things, into the legal categories developed for inherently territorial things, such as land and tangible movables, should be abandoned. Although it would, in principle, be possible to ascribe to crypto assets, private keys, and decentralised ledgers, an artificial *situs*, it is submitted that the extent to which the rules referring to *situs* were developed in respect of specific types of assets will render any application to crypto assets somewhat unsatisfactory and strained.

Instead, it is submitted that new categories and rules based on alternative connecting factors should be developed to accommodate, not only crypto assets, but other assets based on wholly abstract concepts that are similarly omniterritorial and/or which presently lack a *lex creationis*. Such development

127 *Id*., para. 27 (Mance LJ).
128 *Id*., para. 37 (Mance LJ).

is all the more imperative, given the rate and extent to which digital assets gain ever more significance in modern socio-economics.[129] It is worth noting that courts have grappled with localising data and information assets more generally since the advent of the information age in the early 1990s.[130]

Given the omniterritorial nature of such assets, it is clear that any such solution can only plausibly be international in scope.[131] Key issues to be addressed, as identified in this contribution, include the following.

4.3.1 Reforms to National Property Laws

The unavoidable reality is that proprietary claims between private persons will always be brought before national courts which, furthermore, will typically apply *lex fori* in matters of characterisation and where the applicable law is unclear. National property law is, therefore, the starting point for any reform, and this contribution has drawn attention to several aspects of English law that require reconsideration. These have included:

i. recognition of intangible assets that are not properly *choses* in action, *i.e.*, underpinned by an obligation, nor given legal effect through statute and, therefore, presently lack a *lex creationis*;
ii. recognition that, accordingly, Rule 135 of *Dicey, Morris, and Collins* cannot serve as a uniform rule for all intangibles, and alternative rules are required for the type of asset mentioned in subsection (i) above; and,
iii. an appropriate cause of action for vindicating proprietary rights to private keys, recognising the difficulties inherent in ascertaining which copy is definitive for legal purposes.

4.3.2 Clarification on EU Law

In respect of the EU system of PIL, clarification is required, either from the CJEU or legislative amendments, regarding at least:

i. whether a contract for the provision of a crypto asset is one for the 'sale of goods' or 'provision of services' within the meaning under both the Rome I

129 Such as browser-generated information and other similar data produced as a consequence of modern wireless interconnectivity. See, for example, *Vidal-Hall* (n 78) and *Lloyd v Google LLC* [2019] EWCA Civ 1599, especially paras. 46–47 (Vos C).

130 Of particular note are cases involving search warrants in respect of servers. See the discussion of *In re Search Warrant No 16-960-M-01 to Google, In Re Search Warrant No 16-1061-M to Google*, 232 F Supp 3d 708 (ED Pa 2017); and of end-community as a connecting factor in Horatia Watt et al. (eds), *Global Private International Law: Adjudication Without Frontiers* (Cheltenham: Edward Elgar Publishing 2019), 397; 399–400.

131 This is already recognised by working groups within national jurisdictions. See, for example, the UK Jurisdiction Taskforce (n 102), para. 97.

and Brussels I Recast Regulations;

ii. whether crypto assets are an immovable for the purpose of Article 24(1) of the Brussels I Recast Regulation; and

iii. the circularity inherent in characterisation of claims under national law for the purpose of establishing jurisdiction, as aptly demonstrated in cases of joinder under Article 8(1) of the Brussels I Recast Regulation.

4.3.3 An International Solution

Given the omniterritorial nature of crypto assets, it is submitted that the only plausible solution to the issues they pose for PIL would be international in scope. Such international solution would be most effective if drafted in conjunction with reforms to national property laws, as proposed above, following a comparative analysis of such national laws to identify common issues, and potential solutions. Any resulting international solution should, at a minimum:

i. adopt a foundational property analysis of its subject matter to inform and rationalise legal content;

ii. consider whether a new category in addition to immovables, and movables, to accommodate crypto assets and other omniterritorial assets would be appropriate;

iii. determine whether *situs* should be maintained as a connecting factor for establishing jurisdiction and determining *lex causae*, and if so, ascribe to it a definitive *situs*.

5 Conclusions

This contribution began with the proposition that crypto assets and decentralised ledgers pose an 'intractable' problem for PIL in that, by their very nature, they cannot be meaningfully situate in any jurisdiction for the purpose of rules based on *situs.* It considered the rationale of the *lex situs* rule; considered various proposals for a fictional *situs*; and drew attention to the role of the property characterisation of the underlying thing upon which any proposal for a fictional *situs* is necessarily premised.

Part 2 demonstrated that, notwithstanding the difficulty of analysing such assets in the traditional property terms of PIL, the underlying facts of any live dispute before a court will often yield a characterisation in the law of obligations, which, for the purpose of PIL, will not refer to *situs*.

Part 3, however, demonstrated that in some cases, an outright proprietary analysis of the dispute will be unavoidable. In the application of the traditional PIL rules based on *situs*, various problems were highlighted.

Part 4 then contextualised these issues within a broader review of the rules prioritising *situs* to conclude that such rules referring to situs are not absolute; nor are any rules of PIL to be applied rigidly. Accordingly, it was proposed that reforms to national property laws and clarification at EU level to accommodate modern abstract intangible assets are required, which should be ideally taken in conjunction with both (i) a comparative analysis of national property laws; which (ii) would then inform an international solution for the private law aspects of omniterritorial assets.

Such proposal for reforms at national level in conjunction with an international solution in respect of an area of law hitherto widely recognised as falling exclusively within the competence of nation states as a matter of Westphalian concepts of territorial sovereignty, is undoubtedly ambitious. However, a truly concerted effort encompassing comparative approaches to inform both national reform and the drafting of an international instrument is an unprecedented opportunity for maximising harmonisation and minimising fragmentation and difficulties in practice of applying international principles on a domestic level. Accordingly, legislators should not be daunted.

CHAPTER 9

The Law Applicable to Crypto Assets: What Policy Choices Are Ahead of Us?

Burcu Yüksel Ripley and Florian Heindler

1 Introduction

Crypto assets can be defined broadly as cryptographically secured digital representations of value which can be transferred, stored or traded electronically by the use of distributed ledger technology (DLT) or a similar technology. Since their introduction in 2009 with Bitcoin, and particularly in the last few years with their expansion of use in various areas and sectors for different purposes, regulators and legislators at national and international levels have been struggling to catch-up with the development of crypto assets and to adapt their laws to the global paradigm shift represented by the possibilities of crypto assets.

Private law aspects of crypto assets raise various questions including the rights to possess, transfer, pledge, lease, or exclude others from their use. Traditional methods and concepts of private law are challenged by crypto assets due to their novel and complex nature and the cross-border situations they involve. Currently, there is no international regime that governs crypto assets. There are various initiatives in progress for developing international substantive rules, such as the work of the Unification of Private Law (UNIDROIT) and the United Nations Commission on International Trade Law (UNCITRAL).[1] However, due to the novel, complex and fast-evolving nature of crypto assets, and given the difficulties with previous attempts to include crypto assets into the scope of other projects,[2] the development of a harmonised or unified

1 See *e.g.* UNIDROIT, "Digital Assets and Private Law: Study LXXXII - Digital Assets and Private Law Project" (*UNIDROIT*) <https://www.unidroit.org/work-in-progress/digital-assets-and-private-law> accessed 29 June 2023; Matthias Lehmann, "National Blockchain Laws as a Threat to Capital Markets Integration" (2021) 26 Uniform Law Review 148.

2 For example, when preparing the Guide on the Commentary on the UNCITRAL Model Law on Secured Transactions, an interpretative comment saying that the term "money" includes digital currency was agreed to be excluded from the discussion report by the participating states. On this issue, see Stella Galehr and Tessa Grosz, "Discussion report: receivables and securities in private international law" (2019) 24 Uniform Law Review 738.

© BURCU YÜKSEL RIPLEY AND FLORIAN HEINDLER, 2023 | DOI:10.1163/9789004514850_011
This is an open access chapter distributed under the terms of the CC BY-NC-ND 4.0 license.

substantive legal framework on aspects of crypto assets, if possible at all, will likely take time. In addition, potential international substantive law rules in the area are likely to cover only some of the main aspects of crypto assets and require compromise in the scope, which means that they cannot provide a complete legal regime for crypto assets.[3] It is therefore inevitable that there will be questions to be resolved by the applicable national law which is to be determined by either harmonised or unified Private International Law (PIL) rules, if they exist, or PIL rules of the forum.

This emphasises the importance of PIL in this area and of the development of widely accepted PIL rules concerning crypto assets at the international level to enhance legal certainty and predictability in this context. This has been reflected in the current work of the Hague Conference on Private International Law (HCCH) concerning the developments with respect to PIL implications of the digital economy, including DLT and its certain applications including crypto assets.[4]

One of the PIL questions to be addressed is the law applicable to crypto assets. The purpose of this chapter is to critically examine, from a comparative law perspective, some of the key applicable law questions regarding crypto assets, including characterisation, party autonomy under subjective choice of law rules, and the potential objective choice of law rules along with the related issues. The chapter first gives an overview of crypto assets highlighting their key features as well as their diversified and fast-evolving nature in order to assist the choice of law analysis. Building on this foundation, the chapter next addresses challenges around characterisation of crypto assets as money or legal tender, and property, and reflects on the legal implications of this characterisation from a choice of law point-of-view. The chapter then discusses freedom of choice and its operation and limitations in this context, explores considerations around suitable objective connecting factors in the absence of choice and aims to shed light on the possible ways forward in terms of policy choices in determining the law applicable to crypto assets with a view to providing guidance for future work in this fast developing and challenging area.

---

3 Lehmann (n 1).

4 See HCCH, "Developments with respect to PIL implications of the digital economy, including DLT (Prel. Doc. No 4 of November 2020)" (*HCCH*, March 2021) <https://assets.hcch.net/docs/8bdc7071-c324-4660-96bc-86efba6214f2.pdf> accessed 29 June 2023; HCCH, "Proposal for the Allocation of Resources to Follow Private International Law Implications relating to Developments in the Field of Distributed Ledger Technology, in particular in relation to Financial Technology (Prel. Doc. 28 of February 2020)" (*HCCH*, March 2020) <https://assets.hcch.net/docs/f787749d-9512-4a9e-ad4a-cbc585bddd2e.pdf> accessed 29 June 2023.

2 An Overview of Crypto Assets

The idea of crypto assets was put forward in 2008, with the publication of a 9-page white paper on Bitcoin by its pseudonymous founder Satoshi Nakamoto, as "a purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution".[5] Bitcoin, underpinned by blockchain, which is a type of new and revolutionary DLT, was then introduced in 2009 as the first crypto asset to enable the making of non-cash payments with secure digital records being held independently of the usual central trusted authorities, such as banks (*i.e.* without intermediation).[6] In a remarkably short period of time, a global market with thousands of crypto assets has come into existence and continues to grow and evolve.

2.1 *Key Features of Crypto Assets*

There is no universally agreed definition of crypto assets yet. Definitions that have been given thus far are being revisited from time to time and change as necessary as the crypto asset landscape continues to evolve. There is no universally agreed terminology. The term "crypto"[7] and "digital" are sometimes used interchangeably in describing these assets or sometimes the latter is used to refer to a broader category including, but not limited to, the former.[8]

In the European Commission's Proposal for a Regulation on Markets in Crypto-assets (MiCA),[9] the term crypto asset is defined as "a digital

5 Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (*Bitcoin*, 24 May 2009) <https://bitcoin.org/bitcoin.pdf> accessed 29 June 2023.

6 On disintermediation, see *e.g.*, Benjamin Geva, "Banking in the Digital Age - Who Is Afraid of Payment Disintermediation? (European Banking Institute (EBI) Working Paper Series No. 23)" (2018) All Papers 322.

7 The term comes from "cryptography," a technique which is used to ensure security for validation of transactions. See Robleh Ali et al., "Innovations in payment technologies and the emerge of digital currencies" (2014) 54 Bank of England Quarterly Bulletin 262, 263, 266.

8 For an approach which considers crypto assets as a sub-set of digital assets, see *e.g.*, Law Commission of England and Wales, "Digital assets: Call for evidence" (*Law Commission*, April 2021), para. 1.20 <https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/04/Call-for-evidence.pdf> accessed 18 June 2021. For an approach which differentiates crypto assets from other digital assets, see also Jason G. Allen et al., "Legal and Regulatory Considerations for Digital Assets" (*University of Cambridge*, 2020), 13 <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/10/2020-ccaf-legal-regulatory-considerations-report.pdf> accessed 29 June 2023.

9 Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, [2020] COM(2020) 593 final, 2020/0265(COD) ("MiCA Proposal").

representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology".[10] A similar definition can be found in the United Kingdom (UK) Government consultation and call for evidence on the UK Regulatory Approach to Cryptoassets and Stablecoins,[11] which states that "a cryptoasset is understood to be a digital representation of value or contractual rights that can be transferred, stored or traded electronically, and which may (though does not necessarily) utilise cryptography, distributed ledger technology or similar technology".[12]

Based on these definitions, one can identify at least two distinguishing elements of crypto assets. First, they exist only electronically as values and do not have any physical existence. Second, they are underpinned by a DLT or similar technology to securely transfer values and also record and store the values on the ledger within the network. Each network participant has a public key (used to encrypt data) paired with a private key (used to decrypt data), and transactions take place between crypto asset wallets[13] of the participants.[14]

Specific technicalities of the network may differ depending on how the ledger is accessed and updated and by whom. The network can be "permissionless", "permissioned" or a combination of both.[15] In permissionless networks, as is the case with Bitcoin, the ledger is public and can be updated by a consensus of the participants, known as miners or nodes, who act as transaction verifiers and bookkeepers and work in a peer-to-peer network informally formed with no central coordination.[16] There is a high degree of privacy by encryption

10 See *id.*, Article 3(2).

11 HM Treasury, "UK regulatory approach to cryptoassets and stablecoins: Consultation and call for evidence" (*HM Treasury*, January 2021) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950206/HM_Treasury_Cryptoasset_and_Stablecoin_consultation.pdf> accessed 29 June 2023.

12 *Id.*, para. 1.11.

13 According to *id.*, 38, a crypto asset wallet (although its design and particular features may vary) typically allows the storage and management of crypto assets and cryptographic keys to enable the user to store and transfer.

14 Ali et al. (n 7), 268–270, 273–274.

15 See *e.g.*, UK Government Chief Scientific Adviser, "Distributed Ledger Technology: beyond block chain" (*Government Office for Science*, 2015) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf> accessed 29 June 2023.

16 See *e.g.*, Ali et al. (n 7), 266, 268; Committee of Payments and Market Infrastructures Markets Committee of the Bank of International Settlement, "Central Bank Digital Currencies" (*BIS*, March 2018), 97 <https://www.bis.org/cpmi/publ/d174.pdf> accessed 18 June 2021 ("BIS 2018 Report"). This process is done by special purpose-built hardware and involves solving complex algorithmic equations which requires a high amount of computing power. See Ali et al. (n 7), 273–274.

in the network since participants do not disclose their identity.[17] In permissioned networks, the ledger is private and can be updated by trusted participants, known as trusted nodes, under the permission of a central entity which is generally the company that has developed the crypto asset in question.[18]

The distributed ledger, regardless of the type of network, can therefore be understood as a kind of distributed database which includes the entire history of all the transactions that have ever happened within the network and which cannot be modified by a participant secretly as every transaction is recorded together with the history of previous transactions in the ledger.[19] This offers several advantages, including traceability and transparency, privacy, integrity, immutability, verification of receipt, high-level security and immunity, direct peer-to-peer real-time transaction bypassing intermediaries, and, as a result, making trust rather superfluous among the participants of the network.[20]

As the size of the distributed ledger keeps growing substantially every moment with the addition of each new transaction to the ledger, this has led to scalability issues, particularly in permissionless networks, and also the emergence of third-party intermediaries, such as crypto asset wallet providers or crypto asset exchanges,[21] through which participants access and manage their crypto assets.[22] In terms of crypto asset wallet providers, the model can be (i) custodial (known as a "hot" wallet) where the service provider is in full

17 Ali et al. (n 7), 266.

18 BIS 2018 Report (n 16), 96–97; HM Treasury, Financial Conduct Authority (FCA), and the Bank of England, "UK Cryptoassets Taskforce: final report" (*HM Treasury*, October 2018), 10 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf> accessed 29 June 2023 ("UK Taskforce Report").

19 See Riccardo de Caria, "A Digital Revolution in International Trade? The International Legal Framework for Blockchain Technologies, Virtual Currencies and Smart Contracts: Challenges and Opportunities," in UNCITRAL, "Modernizing International Trade Law to Support Innovation and Sustainable Development" (*UNCITRAL*, November 2017), 106 <https://aperto.unito.it/retrieve/handle/2318/1632525/464608/R.%20de%20Caria%2c%20A%20Digital%20Revolution%20%282017%29.pdf> accessed 29 June 2023.

20 See *e.g.*, Burcu Yüksel and Florian Heindler, "Use of Blockchain Technology in Cross-Border Legal Cooperation under the Conventions of the Hague Conference on Private International Law (HCCH)" (*Aberdeen Law School Blog*, 15 August 2019) <https://www.abdn.ac.uk/law/blog/use-of-blockchain-technology-in-crossborder-legal-cooperation-under-the-conventions-of-the-hague-conference-on-private-international-law-hcch/> accessed 29 June 2023.

21 According to the HM Treasury (n 11), 38, a crypto asset exchange is a venue that facilitates the purchase or selling of crypto assets, either in exchange for fiat currencies or other crypto assets.

22 BIS 2018 Report (n 16), 99, 105.

control of keys and assets, generally in the interest of customer convenience when transacting; (ii) non-custodial (known as a "cold" wallet) where the customer is in full control of keys and unilaterally transfers crypto assets; or (iii) hybrid where approval of both the service provider and the customer is required to unlock or transfer crypto assets.[23] In terms of crypto asset exchanges, the model can be (i) centralised where the exchange operator controls matching, clearing, and settlement, (ii) peer-to-peer where the exchange operator connects buyers with sellers for clearing and settlement; or (iii) decentralised where all processes are directly executed on and by the DLT system without a central operator.[24]

As is seen, technical and operational aspects of crypto assets underpinned by DLT or a similar technology significantly differ from those of centralised networks. From a choice-of-law point-of-view, these key features of crypto assets are important to be taken into account, in particular in identifying or developing suitable connecting factors and localising these connecting factors in determining the law applicable to crypto assets.

2.2 *Current Crypto Assets Landscape*

The first crypto asset, Bitcoin, was issued privately (*i.e.* not by a central bank or other central authority of a state), and was originally designed to create an alternative system of payment in the context of the exchange of goods and services. Over the years, with the introduction of other crypto assets with different functions and nature, the crypto assets landscape has been significantly and continuously evolved and diversified.

Although there is no universally agreed classification of crypto assets, based on their functions, crypto assets can be classified via three main categories: exchange tokens, security tokens, and utility tokens.[25] According to the classification by the UK Cryptoassets Taskforce, exchange tokens are crypto assets like Bitcoin that are used as a means of exchange and investment but are not state backed. Security tokens are used for investment and as a capital raising tool. They may provide certain rights such as ownership, repayment of a sum of money or entitlement to a share of future profits. They may also be transferable securities or financial instruments. Utility tokens are also used for investment and as a capital raising tool, and they can be redeemed for access to a specific product or service typically provided using a DLT platform. It is also to

23 HM Treasury (n 11), 38.

24 *Id.*

25 For this classification, see the HM Treasury, FCA, and the Bank of England (n 18), 11–15. For an overview of major token classification frameworks, see Allen et al. (n 8), 10.

be noted that many crypto assets take a hybrid form, falling into different categories at different points in time.[26] For example, they may be initially used to raise capital and fall into the category of security tokens, and later, with changing user behaviour, be used primarily as a means of exchange and fall into the category of exchange tokens.[27]

Another type of crypto assets, the so-called "stablecoins", has also recently emerged as a new category. In contrast to crypto assets like Bitcoin, which are highly volatile, stablecoins (such as Diem, formerly Libra) aim to maintain their value against one or more reference asset, such as fiat currency or a commodity.[28] They are considered to have significant potential of becoming widely accepted globally, in particular in cross-border payments, and are attracting attention in many countries.

Crypto assets issued by central banks, the so called "Central Bank Digital Currencies (CBDC)" are also attracting attention globally and being explored by over 50 monetary authorities,[29] including the Bank of England,[30] the European Central Bank,[31] the Federal Reserve System,[32] the Bank of Canada[33] and the Swiss National Bank.[34]

From a choice-of-law point-of-view, the fast-evolving and diversifying crypto assets landscape is to be taken into account in developing choice-of-law rules. This is not an area where one hard and fast rule could satisfactorily accommodate the needs of the current, and future, crypto assets landscape.

---

26 HM Treasury (n 11), 5.

27 *Id*.

28 On stablecoins, see *id*., Chapter 3; see also the MiCA Proposal (n 9), Explanatory Memorandum.

29 Luca D'Urbino, "The digital currencies that matter: Get ready for Fedcoin and the e-euro" (*The Economist*, 9 May 2021), 11 <https://www.economist.com/leaders/2021/05/08/the-digital-currencies-that-matter> accessed 29 June 2023.

30 Bank of England, "UK central bank digital currency" (*Bank of England*, 13 May 2022) <https://www.bankofengland.co.uk/research/digital-currencies> accessed 18 June 2021.

31 European Central Bank (ECB), "A digital euro" (*ECB*) <https://www.ecb.europa.eu/paym/digital_euro/html/index.en.html> accessed 29 June 2023.

32 Board of Governors of the Federal Reserve System, "FAQs: What is a Central Bank Digital Currency?" (*Federal Reserve*, 20 January 2022) <https://www.federalreserve.gov/faqs/what-is-a-central-bank-digital-currency.htm> accessed 29 June 2023.

33 Bank of Canada, "Digital currencies and fintech: projects" (*Bank of Canada*) <https://www.bankofcanada.ca/research/digital-currencies-and-fintech/projects/> accessed 29 June 2023.

34 Marc Jones, "Swiss central bank readying cross-border digital currency test" (*Reuters*, 29 April 2021) <https://www.reuters.com/article/snb-digitalcurrency-idUSL1N2MM1UX> accessed 29 June 2023.

Choice-of-law rules in this area should offer a sufficient degree of flexibility along with legal foreseeability and certainty to facilitate the crypto assets landscape.

3 Characterisation of Crypto Assets

With respect to choice of law, characterisation is one of the first questions raised in relation to crypto assets. Will they be treated as money or legal tender, or as property? The answer may vary from one jurisdiction to another, and in some jurisdictions, there is no clear answer yet.[35]

3.1 *Crypto Assets as Money or Legal Tender*

Money can have different meanings in different situations.[36] From an economic point of view, it is usually taken that there are three main criteria for something to be considered as money: acting as a medium of exchange, as a store of value and as a unit of account.[37] Acceptance in a community is considered as an element in this analysis.[38]

Legal tender, on the other hand, has a narrower technical meaning than money. Legal tender usually refers to the banknotes or coins that constitute the national currency issued under the legislation of the given state.[39] What is classed as legal tender therefore varies. For example, across the UK, English banknotes are not legal tender in Scotland, and Scottish banknotes are not legal tender in England or Scotland.[40] Foreign currency, unless adopted by a

35 For a comparative study on this matter, see Law Library of Congress and the U.S. Global Legal Research Directorate, "Regulation of Bitcoin in selected jurisdictions" (*Library of Congress*, January 2014) <www.loc.gov/item/2014427360/> accessed 18 June 2021; for different accounts on this topic see Philipp Hacker, Ioannis Lianos, Georgios Dimitropoulos and Stefan Eich (eds), *Regulating Blockchain: Techno-Social and Legal Challenges* (Oxford: OUP 2019) Part II; Primavera De Filippi, "Bitcoin: a regulatory nightmare to a libertarian dream" (2014) 3 Internet Policy Review: Journal on Internat Regulation 1; Georgios Dimitropoulos, "The Law of Blockchain" (2020) 95 Wash. L. Rev. 1117.

36 Charles Proctor, *Mann on the Legal Aspect of Money* (7th edn, Oxford: OUP 2012), para. 1.04.

37 *Id*., para. 1.09.

38 Benjamin Geva and Dorit Geva, "Non-State Community Virtual Currencies," in David Fox and Sarah Green (eds), *Cryptocurrencies in Public and Private Law* (Oxford: OUP 2019), 292.

39 For this definition, see *id*., 285.

40 Bank of England, "What is a legal tender?" (*Bank of England*, 30 January 2020) <https://www.bankofengland.co.uk/knowledgebank/what-is-legal-tender> accessed 18 June 2021; Committee of Scottish Bankers (CSCB), "Legal Position" (*CSCB*) <https://www.scotbanks.org.uk/banknotes/legal-position.html> accessed 29 June 2023.

state as its own, is not legal tender, but can still be considered by law as money without having the legal tender capacity.[41]

Early responses from regulatory authorities in some jurisdictions seem to have indicated a tendency towards not recognising crypto assets as money or currency. In the UK, the Cryptoassets Taskforce assessed that crypto assets are too volatile to be a good store of value; they are not widely accepted as a means of exchange, and they are not used as a unit of account; and, they therefore are not considered to be a currency or money.[42] Similarly, in the EU, the European Central Bank assessed that they do not fit the economic or legal definition of money or currency.[43] As a reflection of this, and probably to avoid any confusion with fiat currencies, the term crypto assets has been preferred to be used by regulatory authorities as opposed to the term cryptocurrencies or virtual currencies. Although early responses from judicial authorities varied on this question,[44] it is asserted that the decisions were given in a particular context and therefore do not represent a general principle or conclusive answer on the question.[45] These early responses are also likely to be re-visited in parallel with the fast-evolving nature of crypto assets and in light of the emergence of new categories of crypto assets.

From a choice-of-law perspective, the importance of this discussion lies in the application of the principle of *lex monetae* and the application of currency as a connecting factor in determining the law applicable to crypto assets. As money traditionally reflects an exercise of sovereignty by states,[46] the issues relating to money and currency are subject to the law of the issuing state (*lex monetae*). The *lex monetae* is deemed to have a broad scope of application that includes, in addition to the meaning of the currency in which the debt is expressed, its form, its nominal value, and also the relationship between

41 Geva and Geva (n 38), 285–286.

42 HM Treasury, FCA, and the Bank of England (n 18), para. 2.13.

43 European Central Bank, "Virtual Currency Schemes - a further analysis" (*ECB*, February 2015), 23–25 <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf> accessed 29 June 2023.

44 See *e.g.*, *Case Skatteverket v. David Hedqvist*, C-264/14, ECLI:EU:C:2015:718; *Securities and Exchange Commission v Trendon T. Shavers and Bitcoin Savings and Trust*, Case No. 4:13-CV-416 (6 August 2013); *United States v. Faiella*, 39 F. Supp. 3d 544 (S.D.N.Y. 2014); *Florida v. Espinoza*, Case No. F14–2923 (Fla. 11th Cir. July 22, 2016).

45 See Rosa María Lastra and Jason Grant Allen, "Virtual currencies in the Eurosystem: challenges ahead" (*European Parliament*, July 2018), 18–21 <https://www.europarl.europa.eu/cmsdata/150541/DIW_FINAL%20publication.pdf> accessed 29 June 2023; Geva and Geva (n 38), 301. More broadly, see also Charles Proctor, "Cryptocurrencies in International and Public Law Conceptions of Money," in David Fox and Sarah Green (eds), *Cryptocurrencies in Public and Private Law* (Oxford: OUP 2019).

46 Proctor (n 36), para. 1.12.

the old currency and the new currency in case of a change.[47] The application of the principle of *lex monetae* in the context of crypto assets is not straightforward.[48] For crypto assets which are not state backed, there seems to be no room for the application of the principle of *lex monetae*, since there is no issuing state whose law could be applied to these types of crypto assets.[49] On the other hand, the newly emerging stablecoins, with value backed by one single fiat currency, and CBDCs, which are issued by central banks of states, would require a different approach, and the principle of *lex monetae* is likely to find a scope of application in relation to these types of crypto assets.

The analogy would be similar regarding the application of currency as a connecting factor in cases concerning crypto assets.[50] For crypto assets which are not state backed, currency as a connecting factor does not establish a link to any country. On the other hand, types of stablecoins referenced against a fiat currency and CBDCs are likely to be capable of establishing such a link between the asset in question and a country in most cases.

As a very recent development, El Salvador, where the US dollar is legal tender, has announced that it plans to adopt Bitcoin as legal tender alongside the US dollar.[51] If this happens, this will make El Salvador the first country in the world to adopt Bitcoin as legal tender. From a choice-of-law perspective, this would initiate a new discussion as regards the application of the principle of *lex monetae* and the application of currency as a connecting factor in cases where the crypto asset in question is privately issued but backed by a state (or more than one state). It is likely that an additional connecting factor or factors would be needed in such cases for the application of the law of that state.

---

47 On *lex monetae*, see *e.g.*, Lord Collins of Mapesbury and Jonathan Harris (eds), *Dicey, Morris & Collins on the Conflict of Laws* (15th edn, Mytholmroyd: Sweet and Maxwell 2012), paras. 37–009, 37–010. The principle of *lex monetae* is also accepted in national PIL rules; see *e.g.*, Article 147 of the Swiss Federal Act on Private International Law (PILA) of 18 December 1987, AS 1988 1776, SR 291.

48 Burcu Yüksel, "International Payments in Virtual Currencies Underpinned by Blockchain: New Challenges for Private International Law" (78th International Law Association Biennial Conference, August 2017), Sydney, Australia.

49 For the *lex monetae* in relation to obligations denominated in Bitcoin or analogous crypto assets, see Andrew Dickinson, "Cryptocurrencies and the Conflict of Laws," in David Fox and Sarah Green (eds), *Cryptocurrencies in Public and Private Law* (Oxford: OUP 2019), 120–121.

50 For the application of currency as a connecting factor for objective choice of law rules in determining the law applicable to electronic funds transfer, see Burcu Yüksel, *Uluslararası Elektronik Fon Transferine Uygulanacak Hukuk* (Istanbul: XII Levha 2018), 172.

51 BBC, "Bitcoin: El Salvador plans to make cryptocurrency legal tender" (*BBC*, 6 June 2021) <https://www.bbc.co.uk/news/world-latin-america-57373058> accessed 29 June 2023.

3.2 *Crypto Assets as Property*

Property and ownership, from a legal point-of-view, can be defined, understood and categorised differently in different jurisdictions. Property law is an area that differs significantly between Common Law and Civil Law, as well as between different Civil Law jurisdictions.[52] Therefore, it is an area in which it is difficult to find a compromise in developing widely-accepted international rules or standards.[53]

Early responses from regulatory authorities as well as judicial authorities in some countries seem to have indicated a tendency towards recognising crypto assets as property in a variety of contexts. In the UK, one of the first regulatory responses came from Her Majesty's Revenue and Customs (HMRC) which stated in one of its policy papers that crypto assets will be considered as property for the purposes of inheritance tax while also noting that it "will look at the facts of each case and apply the relevant tax provisions according to what has actually taken place (rather than by reference to terminology)."[54] This indicated that the legal characterisation and treatment of crypto assets will require a case-by-case analysis in which the type, peculiarities and function of the crypto asset in question will be relevant and taken into account, along with the issue in question. English court judgments suggest so far that crypto assets are, or can be, treated as property within the Common Law definition of the term.[55] These judgments are in line with the view of the UK Jurisdiction Task Force

52 For example, the legal regime in Germany (and in states which adopted the German Civil Code) is very different to the regime of other Civil Law countries; see Maxim Bashkatov et al., "A Comparative Analysis on the Current Legislative Trends in Regulation of Private Law Aspects of Digital Assets (University of Aberdeen School of Law Working Paper Series 004/19)" (*University of Aberdeen*, 2019) <https://www.abdn.ac.uk/law/documents/Yuksel-Ripley-004.pdf> accessed 29 June 2023.

53 This is, for example, reflected in the UNCITRAL, *United Nations Convention on Contracts for the International Sale of Goods* (*Vienna, 1980*) (New York: United Nations Publication 2010) ("CISG"), and in the International Chamber of Commerce, *Incoterms® 2020* (ICC 2020), as neither deals with the effect of the sales contract on the property in the goods sold.

54 For the HMRC's work in the area, see HM Revenue & Customs, "Tax on cryptoassets" (*HMRC*, 30 March 2021) <https://www.gov.uk/government/publications/tax-on-cryptoassets> accessed 29 June 2023.

55 See *e.g.*, *Ion Science Ltd v Persons Unknown* (Unreported, 21 December 2020); Andrew Moir et al., "High Court considers where cryptocurrencies are located and compels disclosure of information by cryptocurrency exchange outside the UK" (*Herbert Smith Freehills*, 24 February 2021) <https://hsfnotes.com/litigation/2021/02/24/high-court-considers-where-cryptocurrencies-are-located-and-compels-disclosure-of-information-by-cryptocurrency-exchanges-outside-the-uk/> accessed 29 June 2023; *AA v Persons Unknown* [2019] EWHC 3556 (Comm).

Statement on Cryptoassets and Smart Contracts under English law[56] and also with the conclusion that was reached in another Common Law jurisdiction, *i.e.* New Zealand, in the case of *Ruscoe v Cryptopia Ltd* (*in liquidation*) [2020] NZHC 782.[57] The tendency towards recognising crypto assets as property is also seen in the US and Singapore.[58]

If crypto assets are regarded as property, the next issue would be their classification and treatment in a given property law framework. In general, a distinction is made between real property and personal property in Common Law, corresponding to immovable property and movable property in Civil Law, and between tangible property (*e.g.* physical things) and intangible property (*e.g.* intellectual property) mirroring *choses* in possession and *choses* in action in Common Law.[59] The traditional understanding of property, as well as ownership in law under this categorisation, is challenged in the context of crypto assets due to their unique nature.[60] They are a form of intangible property, meaning that they do not have a physical existence, but they also share several characteristics with tangible property such as transferability and storage.[61] Furthermore, the fact that the transfer of title to a crypto asset does not involve physical objects blurs the boundaries between proprietary and obligatory rights.[62]

From a substantive law point-of-view, it is important to note the traditional discussion that exists relating to the question about the nature of property law

56 UK Jurisdiction Task Force, "Legal Statement on Cryptoassets & Smart Contracts" (*Tech Nation*, November 2019), 21–22 <https://technation.io/lawtech-uk-resources/#cryptoassets> accessed 29 June 2023.

57 Moir et al. (n 55).

58 See Allen et al. (n 8), 21–22.

59 See *e.g.*, Jonathan Hill and Máire Ní Shúilleabháin, *Clarkson & Hill's Conflict of Laws* (5th edn, Oxford: OUP 2016), 470–472.

60 For English Common Law position, see Law Commission of England and Wales (n 8), 6–9. On this issue, see also David Fox, "Cryptocurrencies in the Common Law of Property," in David Fox and Sarah Green (eds), *Cryptocurrencies in Public and Private Law* (Oxford: OUP 2019); Daniel Carr, "Cryptocurrencies as Property in Civilian and Mixed Legal Systems," in David Fox and Sarah Green (eds), *Cryptocurrencies in Public and Private Law* (Oxford: OUP 2019); Kelvin FK Low and Wu Ying-Chieh, "The Characterisation of Cryptocurrencies in East Asia," in David Fox and Sarah Green (eds), *Cryptocurrencies in Public and Private Law* (Oxford: OUP 2019).

61 Financial Markets Law Committee, "FinTech: Issues of Legal Complexity" (*FMLC*, June 2018), 20–21 <http://fmlc.org/wp-content/uploads/2018/06/FinTech_bound.pdf> accessed 18 June 2021; Joanna Perkins and Jennifer Enwezor, "The legal aspects of virtual currencies" (2016) 10 Butterworths Journal of International Banking and Financial Law 569, 570.

62 See Florian Heindler, "The law applicable to third-party effects of transactions in intermediated securities" (2019) 24 Uniform Law Review 685, 696.

either as a right which is characterised mainly by *erga omnes* entitlements and, therefore, in principle applies to tangibles and intangibles, or as a subjective right which is connected with a particular power in relation to goods.[63] From a choice-of-law point-of-view, this discussion raises the question as to whether intangibles, such as crypto assets, should be characterised as obligations or whether choice-of-law rules for property law should be applied to them.

One of the important aspects of this discussion lies in the application of *lex situs*, *i.e.* the law of the country where the property is located, in determining the law applicable to crypto assets. *Lex situs* frequently applies in international property law.[64] However, its application to crypto assets is not straightforward as crypto assets are not located in one single place, at least not in many cases where the ledger is distributed or decentralised with a cross-border nature. The English High Court recently considered for the first time the location of a crypto asset in *Ion Science Ltd v Persons Unknown*[65] and reached the view that the location of a crypto asset (in the given case Bitcoin) is the place where the person or company who owned the coin or token is domiciled.[66] Although this decision helps to bring some clarity to the issue, it leaves room for a debate on the suitability of the application of *lex situs* in its traditional understanding in the context of crypto assets which do not have a situs as such. As will be explored in Part 5 below, this raises the question as to whether proprietary aspects of crypto assets should be governed by the law applicable to obligations or by newly adopted choice of law rules. Whether the network is permissionless or permissioned can make a difference in developing a suitable connecting factor in this context as well, since, particularly for the former, the application of a single law could be preferred over splitting the applicable law based on the location of participants.

4 Defining the Scope of Choice-of-Law Rules or Instruments

Particular matters relating to the scope of application require specific attention to inform policy choices in defining an adequate choice-of-law framework

63 See the discussion in Claus-Wilhelm Canaris, "Die Verdinglichung obligatorischer Rechte," in *Festschrift für Werner Flume* (Köln: Schmidt 1978), 371. Since then, the arguments have not changed considerably.

64 See recently, Caroline Rupp, "lex rei sitae reloaded," in Florian Heindler (ed), *Festschrift 40 Jahre IPRG* (Wien: Jan Sramek Verlag 2020), 309, 310.

65 See (n 55).

66 It is stated in Moir et al. (n 55), that the court was assisted by the analysis of Dickinson (n 49).

for crypto assets. This includes the adoption of technological neutrality to accommodate future technological innovation and varieties between the legal systems, and to raise awareness of the existing PIL landscape, in particular the prospective interplay of a newly developed choice-of-law rule with choice-of-law rules which are already being applied to neighbouring aspects.

4.1 *Technological Neutrality*

The key to the scope of a specific choice-of-law rule or instrument are the legal terms used to describe the scope of the rule or instrument. The relevant terms in a choice-of-law rule or instrument must be broad enough to encompass the varieties stemming from the diversity of legal systems coordinated by the choice-of-law rule or instrument. It is, therefore, inevitable that the terms defining the scope must be broader than the terms of the substantive law rule of a specific jurisdiction. If the choice-of-law rule or instrument describes its scope with the same narrow terms as in the respective substantive law of the forum, the choice of law rule or instrument cannot be applied to refer equally to an applicable foreign law differing from the substantive law of the forum. This must be avoided particularly if the choice-of-law rule or instrument would be one with universal application such as in the meaning of Article 2 of the Rome I Regulation.[67] This particularity of choice-of-law rules in contrast to substantive law rules is one of the reasons why the decisive terms defining the scope of the choice-of-law rule or instrument must be sufficiently broad.

The second element to be observed is the fast technological progress made in connection with digitalisation. In various fields of cross-border legal interaction, an argument made in favour of technological neutrality is the avoidance of situations where a rule drafted against the background of a specific technological innovation (*e.g.* email) quickly becomes outdated.[68] In the field of PIL, this observation has also been stressed in the recent work of the HCCH on PIL implications for the digital economy.[69] In the field of substantive law, the American Law Institute (ALI) and Uniform Law Commission (ULC) Joint Committee on the Uniform Commercial Code and Emerging

67 Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), [2008] OJ L177/6 ("Rome I Regulation").

68 See, with further references, Florian Heindler, "The digitisation of legal co-operation – reshaping the fourth dimension of private international law," in Thomas John, Rishi Gulati and Ben Köhler (eds), *The Elgar Companion to The Hague Conference on Private International Law* (Cheltenham: Edward Elgar Publishing 2020), 428–429.

69 HCCH, "Developments" (n 4), para. 2.8.

Technologies[70] has most recently emphasised the importance of technological neutrality in substantive law by refraining from giving any references to DLT or other specific technologies and instead using the electronically neutral functional term "controllable electronic record" to encompass future technological innovation. Similarly, the UNCITRAL for its recent Model Law has preferred to use the term "electronic transferable record" and defined it without giving a reference to any specific type of technology such as DLT or blockchain.[71] This is in contrast to the EU's MiCA Proposal and the UK Government's consultation papers concerning crypto assets.[72]

In light of the above analysis, the scope of a choice-of-law rule or instrument should be technologically neutral (first requirement) and broad enough to encompass technological differences in various legal systems (as opposed to being workable for particular legal systems only with the inclusion of specific terms of substantive law) (second requirement). Therefore, the reference to DLT and blockchain in the Council document of the HCCH Permanent Bureau[73] is better to serve only as guidance in developing a rule or instrument; otherwise, the first requirement would not be satisfied.

Moreover, the terms used to define the scope of a choice-of-law rule or instrument should include the functionalities of the phenomenon, mainly those which represent the core for the transactions executed by the involved parties. As observed above,[74] the so-called crypto assets consist of cryptographically secured digital representations of value that can be transferred, stored, or traded electronically by the use of DLT. The special feature of crypto assets is their unique use in a system which, from a purely factual perspective, assigns particular electronic values to a particular person or a particular group of persons and thereby enables the possession-like[75] attribution of digits to a particular person or group. Although the consequences of the control of particular electronic values are extremely diverse, the fact that a certain value is assigned to a particular person or group constitutes a general feature. It is, therefore,

---

70 Uniform Law Commission, "Uniform Commercial Code and Emerging Technologies" (*ULC*,2021)<https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=36a12016-c502-2458-d6a0-0dbe3fddaff7&forceDialog=0> accessed 29 June 2023.

71 UNCITRAL, *UNCITRAL Model Law on Electronic Transferable Records* (New York: United Nations Publications 2017); on technological neutrality, see *id.*, Recital 18 of the Article-by-article commentary.

72 On this issue, see *supra* Part 2.1.

73 HCCH, "Developments" (n 4).

74 See *supra* Part 1.

75 See Article 11 of UNCITRAL (n 70) and its Explanatory Note, para. 13, 105–109.

convincing to consider crypto assets as digital data or electronic values which can be attributed to a particular person or group.

So far as certain types of attributable electronic values can already be classified under the existing choice-of-law rules or instruments (such as financial instruments or electronic money), they should be excluded from the scope of newly developed choice-of-law rules on crypto assets. Further exclusions would be a matter of policy choices. Nevertheless, it seems to be less cumbersome to start with a broad notion of attributable electronic values and provide exceptions, rather than to start with a very narrow definition or complex taxonomy which is better suited to be the focus of a substantive law framework.[76]

4.2 *Different Legal Aspects of Crypto Assets and Scope Rules*

Crypto assets are real-life phenomena which have a potential impact on a large scale of different legal transactions and legal situations.[77] They also raise cross-sectional issues, giving rise to legal questions in the context of family law, particularly the financial aspects of family law, successions law, contract law, tort law, intellectual property law, insolvency law and property law. Therefore, it is important that a choice-of-law framework in this area coordinates the interplay with other choice-of-law rules and instruments.

4.2.1 Crypto Assets as Representations

Crypto assets, defined as attributable electronic values, can be used as representations of contractual and non-contractual claims or of physical objects (*e.g.* tokenised ownership rights in cars). Whether the possession of respective crypto assets (token) leads to ownership of the tokenised object is a question of substantive law.[78] In cases where the ownership and transfer of physical objects or the assignment of rights or claims is already governed by other conflict-of-laws rules, they are to be excluded from the scope of a newly-developed choice-of-law rule or instrument.

The same is true if tokens no longer qualify as crypto assets. In other words, a choice-of-law rule or instrument on attributable electronic values should only refer to the transfer of the attributable electronic values itself and not to

76 See the references in HCCH, "Developments" (n 4), para. 9.

77 See Susanne Gössl, "IPR and Smart Contracts," in Thorsten Voß (ed), Recht der FinTechs (De Gruyter 2023, forthcoming).

78 See *e.g.*, Steven Harris, "Memorandum to the Committee on the Uniform Commercial Code and Emerging Technologies: Controllable Electronic Records" (*UCC*, 18 April 2021) <https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=cdb4e8dd-84ed-8fc6-f579-f0a8280527 4f&forceDialog=0> accessed 29 June 2023.

the transfer of an embodied right or physical token. Therefore, all questions relating to the nature and content of the embodied right are to remain outside the scope of application. This view is supported via an analogy to the scope of choice-of-law rules on intermediated securities. For example, the nature and existence of rights embodied in the security are outside the scope of choice-of-law rules for the proprietary aspects of transactions in intermediated securities in the Hague Securities Convention.[79]

4.2.2 Interplay in the Existing Choice-of-Law System

It is important that situations involving crypto assets are accommodated within the existing choice-of-law system under choice-of-law rules and instruments being applied by courts and tribunals in various fields. This means that, for example, an insolvency regulation cannot be rendered inapplicable just because crypto assets are involved in the case. A corporation purchasing crypto assets still operates under the legislation referred to by *lex societatis*. The statutist framework of choice of law continues to exist and the questions arising in connection with crypto assets must be addressed within this system.[80] A stand-alone solution to address all issues arising across various fields of law in connection with crypto assets does not seem feasible. Moreover, a choice-of-law rule or instrument on crypto assets should only deal with specific questions which are not sufficiently addressed by the existing choice-of-law rules or instruments. Other matters, such as the determination of the law applicable to the operational matters of a company issuing crypto assets or the law applicable to the question of who the legal successor of inheritance (including crypto assets) is, are not questions for a newly developed rule or instrument concerning crypto assets. The crypto community will therefore need to be ready for the complexity to arise by the application and interplay of different choice-of-law rules for situations involving crypto assets. There will be no PIL one-stop-shop for such situations.

It is well understood that complexities arising from a constantly refined and progressively growing nuanced choice-of-law framework, in particular regarding incidental questions, leads to fragmentation and creates challenges. More specifically, the lack of binding rules addressing incidental questions

79 Convention of 5 July 2006 on the Law Applicable to Certain Rights in Respect of Securities held with an Intermediary ("Hague Securities Convention"). The Convention also provides for a limited freedom to choose the applicable law.

80 See *e.g.*, Matthias Lehmann, "Who Owns Bitcoin: Private law Facing the Blockchain," (2020) 21 Minnesota Journal of Law Science & Technology 93, 132–133, regarding inter alia applying the choice of law rules for unjust enrichment in case of an erroneous transfer.

could increase the number of situations in which the applicable law cannot be clearly determined *ex-ante*. It is, therefore, vital to create a concise choice-of-law rule or instrument, which avoids further characterisation within the domain of attributable electronic values and keeps the scope rule technologically neutral and broad. The analysis of the existing choice-of-law rules and instruments should provide for a narrow gap of questions which have not yet been sufficiently addressed to keep the add-up to the existing and already complex choice-of-law framework as concise as possible.

One of the main exclusions from the scope of a choice-of-law rule or instrument is to be the title to acquire an attributable electronic value. Thus, a sales contract or disposition upon death by virtue of which electronic values ought to be transferred to another person is to be governed by the relevant choice of law rules or instruments on contract or succession respectively. Basically, this leads to a choice-of-law rule or instrument aiming at the bundle of rights relating to the crypto assets and their acquisition. These questions are typically connected to the notion of property (*e.g.* rights to use, to allow others to use, to prevent others from using (*i.e.* exclude), to extinguish, *etc.*). They address important preliminary questions in, for example, insolvency law, successions law and family law connected with the aforesaid rights. The important interplay of the different choice-of-law rules with the rule governing proprietary effects should therefore fall into the scope of existing rules in those areas. This means that connecting factors in choice-of-law rules of those areas remain untouched and this would reduce fragmentation in the applicable law. It is, thus, possible to identify, to a large extent, the domain of proprietary questions as a field of law which requires specific legislative intervention for choice-of-law rules or instruments on crypto assets.

5 Policy Choices in Developing Suitable Connecting Factors

Building on the analysis in the previous parts of this chapter, it is useful to make some preliminary points in exploring options for suitable connecting factors in determining the law applicable to crypto assets. In terms of monetary aspects, since money can be legally classified as circulating credit,[81] characterisation of crypto assets used as a payment device can raise, apart from the application of *lex monetae*, the issues of assignment and, in a broader sense and similar to

81 See, with further references, Andreas Rahmatian, *Credit and Creed: A Critical Legal Theory of Money* (London: Routledge 2020), 232; for a complete discussion on the *lex monetae*, see *supra* Part 3.1.1.

other payment schemes (*e.g.*, credit cards), contractual obligations. In terms of proprietary aspects, the acquisition of proprietary rights in crypto assets could be qualified as a question of the law of obligations for choice of law purposes[82] given the challenges around the application of *lex situs* in the context of crypto assets. Different connecting factors might, therefore, be potentially relevant depending on specific uses or functions of crypto assets. This part of the chapter does not, however, take an approach of examining the connecting factors individually under certain categories of issues. It rather aims to shed light on some common considerations that might be taken into account in developing suitable connecting factors for crypto assets across different issues to which they might give rise.

Various connecting factors are currently being explored for determining the law applicable to crypto assets.[83] Different policy choices include considerations around freedom of choice, alignment with the forum of the competent regulatory body (also sometimes referred to as deemed election)[84] if there is one, rules based on the place of record and account keeping (which are linked to the choice-of-law rules on financial instruments),[85] rules used for the issuance of securities for contractual obligations, and, finally, traditional rules on the law applicable to proprietary rights in physical objects.

5.1 *Freedom of Choice*

Freedom of choice usually refers to the choice of law made by parties to a transaction and finds its origin in the well-established principle of party autonomy.[86] This suggests that the parties can agree on the law governing their relationship.

Freedom of choice is an attractive option for a choice-of-law rule regarding crypto assets for a variety of reasons. First of all, parties' choice will be respected under the principle of party autonomy. Secondly, if the freedom of choice is not adopted in this area, the determination of the applicable law based on the objective choice-of-law rules will be extremely complex and some traditional connecting factors in use, such as *lex rei sitae*, will not be straightforward to apply to crypto assets given that these assets do not have a physical

82 See the statements in the discussion report by Galehr and Grosz (n 2), 742.

83 For an overview, see HCCH, "Developments" (n 4), Annex I.

84 For an overview, see *id.*, 8–9.

85 See European Commission, "FISMA Targeted consultations on the review of the Directive on settlement finality in payment and securities settlement systems and on the review of the Financial Collateral Directive" (*EC*, 2021) <https://ec.europa.eu/info/consultations/finance-2021-settlement-finality-review_en> accessed 18 June 2021.

86 See generally Symeon C. Symeonides, *Codifying Choice of Law Around the World: An International Comparative Analysis* (Oxford: OUP 2014) Chapter 3.

location. As the HCCH Permanent Bureau puts it, "DLT and blockchain do not recognise traditional national borders and have global reach."[87] In addition, freedom of choice will also reduce complex interpretation of choice-of-law rules based on, for example, habitual residence, which is particularly difficult in a pseudonymous crypto environment. In permissioned networks, this approach can also ensure the application of single law across the network and allow certain stakeholders, for example creators of a certain technology or type of crypto asset, to determine the applicable law.[88]

However, there are certain limitations to the application of party autonomy in this context, including ambiguities around what is meant by the parties.[89] In addition, there may be issues around the protection of third parties in case of an unlimited freedom of choice. If parties to a specific transaction have the right to choose the law applicable to *erga omnes* effects of their transaction, they could execute their choice to adversely affect or interfere with acquired rights of third parties. Therefore, the general principle that freedom of choice between parties to a specific transaction shall not prejudice the rights of third parties has to be respected. In addition, the application of party autonomy is likely to result in the fragmentation of law within one system unless the choice is made by a central stakeholder and extends to the respective class of assets or systems.[90]

5.2 *Applicable Law in the Absence of Choice*

In cases where there is no choice of law by the parties, the law applicable to crypto assets will be determined according to the objective choice-of-law rules. There are different methods used in different jurisdictions in determining the applicable law in the absence of choice. In the context of crypto assets, some considerations deserve special attention.

5.2.1 Record and Account Keeping

The Hague Securities Convention and the EU directives including choice-of-law rules for intermediated securities[91] contain objective connecting factors

87 HCCH, "Proposal" (n 4), 2.

88 The HCCH refers to it inter alia as the *lex digitalis*, see, HCCH, "Developments" (n 4), Annex I 10.

89 On the limitations of party autonomy in the context of international electronic funds transfers, see Yüksel (n 50), 166–168.

90 See HCCH, "Developments" (n 4), Annex I 9.

91 Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems, [1998] OJ L166/45; Directive 2002/47/EC of the European Parliament and of the Council of 6 June 2002 on

which, broadly speaking, refer to the law of the account keeping credit institution's location. Indeed, the Convention and the EU directives address similar questions as debated herein, since they focus on proprietary questions and include non-tangibles, in particular undocumented book-entry securities.[92] They build on the regulatory environment providing for central gatekeepers acting as intermediaries.[93] Therefore, as it has been often said, it is difficult to imagine a similar approach to be applied to de-centralised crypto assets stored in permissionless networks with no intermediary or service provider.[94] On the other hand, as regards the permissioned networks, there are still attempts to create an analogous rule with reference to the primary residence of the encryption private master keyholder (PREMA) and the place of the relevant operation authority/administrator (PROPA).[95] However, in contrast to an intermediary subject to prudential supervision, so far, there is a lack of transparency in the trading of crypto assets, which makes it difficult to determine who the relevant operation authority/administrator is and where it is located.[96] The location of the private master key raises similar difficulties.

In case of a traceable system which allows the identification of an account keeper, the approach that the Convention and EU directives adopt seems sensible. It is not a continuation of the *lex rei sitae* or *lex cartae sitae*, but a workable connecting factor which is determinable and which cannot be easily manipulated.[97] Therefore, it provides legal certainty, as also stressed by the HCCH.[98]

---

financial collateral arrangements, [2002] OJ L168/43; Directive 2001/24/EC of the European Parliament and of the Council of 4 April 2001 on the reorganisation and winding up of credit institutions, [2001] OJ L125/15.

92 Florian Heindler, "§ 33a IPRG" in Peter Rummel and Meinhard Lukas (eds), *ABGB* (4th edn, Vienna: Manz 2022, forthcoming), para. 8; Matthias Lehmann, *Finanzinstrumente* (Tübingen: Mohr Siebeck 2009), 497.

93 Hubert de Vauplane, "Blockchain and intermediated securities" (2018) 36 Nederlands Internationaal Privaatrecht 94, 102.

94 Michael Ng, "Choice of law for property issues regarding Bitcoin under English law" (2019) 15 Journal of Private International Law 315, 330; Gerald Spindler, "Fintech, digitalization, and the law applicable to proprietary effects of transactions in securities (tokens): a European perspective" (2019) 24 Uniform Law Review 724, 731; Christiane Wendehorst, "Digitalgüter im Internationalen Privatrecht" (2020) 40 Praxis des Internationalen Privat– und Verfahrensrechts 490, 497.

95 Financial Markets Law Committee (FMLC), "Distributed Ledger Technology and Governing Law: Issues of Legal Uncertainty" (*FMLC*, March 2018), 17–18 <http://fmlc.org/wp-content/uploads/2018/05/dlt_paper.pdf> accessed 29 June 2023.

96 See HCCH, "Developments" (n 4), Annex I 9.

97 Heindler (n 62), 694.

98 See HCCH, "Developments" (n 4), Annex I 9.

5.2.2 One System – One Law

From a choice-of-law point-of-view, there are advantages if one single law applies to a network facilitating various transactions between different participants.[99] The idea that one trading system should be subject to a single law is reflected in, for example, Article 4(1)(h) of the Rome I Regulation. According to that provision, "a contract concluded within a multilateral system which brings together or facilitates the bringing together of multiple third-party buying and selling interests in financial instruments, as defined by Article 4(1), point (17) of Directive 2004/39/EC, in accordance with non-discretionary rules and governed by a single law, shall be governed by that law". The same idea prevents the application of consumer protection as per Article 6(4)(e) for contracts concluded within such a system. Substantive law, however, might still provide rules to protect consumers. The one system-one law idea has also been reflected in the use of an escape clause for the transactions consisting of linked contracts, such as guarantee, reinsurance, letter of credit and electronic funds transfer.[100]

Although this analysis is regarding contractual obligations, it can be argued that, within one trading system, the different types of proprietary entitlements should be made subject to one law to avoid confusion. However, it is to be noted that a trading system can accommodate different types of proprietary entitlement, for example different security rights governed by different laws. In addition, the applicable law could also change, for instance with the transfer of a crypto asset. It, therefore, seems more convincing that the attribution of crypto assets in the system is comparable with possession. Holding a crypto asset within the trading system does not mean being the owner, *i.e.* being the holder of a valid title. The applicable law of proprietary aspects can still determine the diverse bundles of rights of the various holders of crypto assets and the applicable law of obligations can determine whether a holder is obliged to hand over the asset to another person because of a pledge or sales agreement. The system can accommodate the legal duties of participants, regardless of whether their obligations to transfer result from a contract concluded under for example French law or Austrian law. In contrast, divergent rules from different jurisdictions about *bona fide* acquisitions, presumption of ownership or good faith, and the requirement that the transferor was the legal owner cannot be easily brought together within one trading system.

99 For this approach regarding international electronic funds transfer, see *e.g.*, Yüksel (n 50), 175–177.

100 On this issue, see *id.* 157–165.

Another situation worth noting is the one addressed for example in Article 6(4)(d) of the Rome I Regulation. The provision excludes the application of consumer protection for "rights and obligations which constitute a financial instrument and rights and obligations constituting the terms and conditions governing the issuance or offer to the public and public take-over bids of transferable securities, and the subscription and redemption of units in collective investment undertakings". The idea behind this exclusion is that those matters should be governed by a single law which is determined by the issuer on the basis of Article 3 of the Rome I Regulation. Consequently, the obligations of the issuer with respect to one class of assets, for example bonds issued under a certain programme, are governed by the same law. In cases where the conflict rule is limited to proprietary effects and excludes questions of title, there will be no need for the protection of consumers through choice-of-law rules either. The contract to acquire crypto assets should be governed by the *lex contractus*[101] which can foresee mechanisms for the protection of weaker parties. A respective choice made by the issuer cannot be overturned by a subsequent choice between the parties of a secondary market transaction, so that the rights of third parties are not negatively affected. The choice is communicated no later than the obligation arises. Similarly, the issuer of a certain class of crypto assets could determine the law governing the proprietary effects of the respective crypto asset. Such a choice made by the issuer of a certain class of crypto assets would govern the proprietary effects of all future transactions regarding a crypto asset out of the respective class. A fall-back rule could refer to an objective connecting factor related to the issuer in the absence of a choice, such as the habitual residence of the issuer. For the purpose of crypto assets, the reference to the creator of the assets, functionally comparable with an issuer of securities, finds its expression particularly in the PResC rule referring to the primary residence of the coder.[102]

The law applicable to the creation of the asset determines the content of the asset (referred to in German as *Wertpapierrechtsstatut* in securities law). Issuing a uniform class of crypto assets requires that the content of the issued class of crypto assets is governed by the same law. In contrast, trading with these assets (referred to in German as *Wertpapiersachstatut* in securities law) could be subject to different laws. Thus, parties can trade different crypto assets governed by different laws in a single transaction or hold these assets in one account.

101 Lehmann (n 80), 132.

102 FMLC (n 95), 21.

5.2.3 Aligning (Regulator's) Forum and Law

The most common method of aligning forum and law is the application of the *lex fori* rule.[103] The application of the law of the state for which protection is claimed (*i.e. lex loci protectionis*) most frequently leads to the application of the *lex fori* as well. The *lex loci protectionis* is widely acknowledged in international intellectual property (IP) law.[104] Intuitively, it may seem preferable to extend the connecting factor for intellectual property rights to crypto assets.[105] However, apart from being well-suited to determine the applicable law for intangibles which cannot have a physical location, the application of the *lex loci protectionis* is based on the ideal of national preferences regarding the protection of intellectual property. It allows states to grant exceptions from the protection and to set conditions under which protected content could be used. The connecting factor is, therefore, deeply rooted in the industrial policies of nation states.[106] Accordingly, both rules have weaknesses in the recognition of title in crypto assets acquired elsewhere. On the other hand, it would be a policy choice to create territorially restricted licence systems over crypto assets and to introduce crypto assets which can be traded solely under the law of a specific jurisdiction. Similar to IP rights, a state could thereby control the acquisition of proprietary rights in crypto assets.[107] This would imply a reasonable threat for the trade in crypto assets and eliminate the current mechanisms. The application of the *lex loci protectionis* or *lex fori*, however, would be well-suited to determine the specific content of the right to a crypto asset. It is not the acquisition and termination of the right as such which should be subject to the law of the forum or the law of the state in which protection is sought, but merely the content of the right acquired under a given contract.[108]

---

103 See *e.g.*, Anton Zimmermann, "Blockchain-Netzwerke und Internationales Privatrecht – oder: der Sitz dezentraler Rechtsverhältnisse" (2018) 38 Praxis des Internationalen Privat– und Verfahrensrechts 566, 573.

104 See *e.g.*, European Max Planck Group on Conflict of Laws in Intellectual Property, "Principles on Conflict of Laws in Intellectual Property" (*CLIP*, 1 December 2011), Art. 3:102 <https://www.ip.mpg.de/fileadmin/ipmpg/content/clip/Final_Text_1_December_2011.pdf> accessed 29 June 2023: "The law applicable to existence, validity, registration, scope and duration of an intellectual property right and all other matters concerning the right as such is the law of the State for which protection is sought."

105 See *e.g.*, Spindler (n 94), 737; Wendehorst (n 94), 495.

106 See, with further references, Florian Heindler, "Der kollisionsrechtliche Schutz digitaler Inhalte aus urheberrechtlicher Sicht," in Caroline S. Rupp (ed), *IPR zwischen Tradition und Innovation* (Tübingen: Mohr Siebeck 2019), 146–148.

107 See Heindler (n 92), para. 22.

108 On the distinction in Austrian and German international property laws, see Florian Heindler, "Continuation of security rights in movable assets in conflict of laws – Austrian approach reconsidered" (2019) 8 European Property Law Journal 301, 303–306, 313–316.

Another method could be seen as a modification of the traditional *lex fori* approach. Instead of referring to the law of the state in which the relevant court is located, a choice for the regulator's forum can imply that the law of the state in which the competent supervisory authority is located would be the applicable law. If the substantive law allows registration under a certain jurisdiction, the connecting factor will further imply a *lex registrationis* principle.[109] However, a permissionless decentralised system does not have a *situs* as such and therefore cannot be addressed satisfactorily by the given choice-of-law rule.[110]

5.3 *Subsequent Occurrences*

In many jurisdictions, the law applicable to the acquisition of property remains unaffected if the location of an asset or other facts of the case determinative for the selection of a particular legal order change after the asset has been acquired. Subsequent occurrences, in other words, do not affect transactions which are already completed. This is said with regard to the determination of the person having a title over an object and their acquisition and loss of property rights. On the other hand, the content of the right *in rem*, subject to *numerus clauses*, is usually determined in accordance with the most current location of the object. The same rule applies to IP law. Similarly, the EU proposal on the law applicable to the third-party effects of assignments of claims[111] defines the relevant time ("time of the conclusion of the assignment contract") and, thus, excludes the impact that subsequent occurrences would otherwise have on the applicable law. This rule, disregarding subsequent occurrences, has a direct connection with the logic of substantive property law, *i.e.* availing and protecting *erga omnes* entitlements across borders. If, following the above motivation, such *erga omnes* entitlements are the focus of a choice-of-law rule or instrument, similar reasoning will be required. This is even the case regarding parties' freedom of choice.[112]

The ratio of protecting *erga omnes* entitlements, thus, requires a stable connecting factor and, accordingly, the respective determination of the relevant time. It excludes the possibility of referring to the applicable law as determined by the connecting factor at the time when a case is pending at a court or when

109 See Sarah Green and Ferdisha Snagg, "Intermediated Securities and Distributed Ledger Technology," in Louise Gullifer and Jennifer Payne (eds), *Intermediation and Beyond* (Oxford: OUP 2019), 352.

110 The problem seems to have addressed in substantive law by transitional provisions in the EU (*e.g.*, Article 123 of the MiCA Proposal (n 9)).

111 Proposal for a Regulation of the European Parliament and of the Council on the law applicable to the third-party effects of assignments of claims, [2018] COM/2018/096 final, 2018/0044(COD).

112 See *supra* Part 5.1.

a suit is submitted to a court. It seems preferable to apply the connecting factor at the time when the activities in question took place.

6 Conclusion

Crypto assets, underpinned by DLT or a similar technology, introduce new challenges to various areas of law, including PIL, due to their novel, complex, fast-evolving and cross-border nature. In light of the global paradigm shift represented by the possibilities of crypto assets, what is at stake is adapting and reforming laws as necessary for a developing global system facilitated by the use of digital innovation. This would arguably be a more challenging task in PIL, compared to substantive law, as demonstrated by the difficulties with previous attempts on reaching a consensus on PIL aspects of technology-driven concepts including crypto assets.

The law applicable to crypto assets is a question that is at the heart of this challenge. The analysis in this chapter suggests that new approaches are needed in interpreting and applying the traditional concepts of choice of law in the context of cyrpto assets. This requires a good understanding of technological aspects of crypto assets and their continuously evolving and diversifying nature across different fields. Some of these approaches will be informed by the developments in substantive law, including characterisation of crypto assets as money or legal tender, or property or as another category. In terms of defining the scope of application of a choice-of-law rule or instrument in this area and in finding suitable connecting factors, the analysis in this chapter suggests the adoption of technological neutrality, and the consideration of existing and future interplay between crypto assets and their use in other fields of law to be important factors to be taken into account. It is also important that the PIL community keeps the dialogue open and ensures international collaboration in finding workable and widely acceptable solutions for challenges raised by crypto assets globally.

CHAPTER 10

The Law Applicable to Digital Representations of Off-chain Assets

Emeric Prévost

1 Introduction

Tokens will undoubtedly become increasingly popular as the model of a "tokenised economy" develops. Simply put, a "tokenised economy" or the "tokenisation" of the economy refers to the phenomenon of asset transformation from "classical" assets (wines, cars, houses, gold, songs, music, shares, bonds, *etc.*) into tokens, which are fundamentally the encoded and transferable representation of one or more rights on a distributed ledger. To gauge the fast growth of the token economy, one could think of the massive fundraising of some Financial Technology (FinTech) start-ups such as the French company Sorare, which managed recently to raise approximately 580 million euros to foster its "fantasy football" business, *i.e.* the issuance and trading of collectible digital cards representing soccer players and matching the real-life performances of each player in the form of non-fungible tokens (NFTs).[1] An NFT is simply a unique set of data encoded on a distributed ledger such as the blockchain (hereinafter generally referred to as "DLT"), which allows for the tracking of the owner of the encoded items. Besides the rights attached to an NFT (*e.g.* access to a service or product, royalties, *etc.*), the authenticity and scarcity of each single NFT make them potentially extremely valuable. In March 2021, the NFT card of Cristiano Ronaldo was, for instance, sold on the Sorare platform for 150 Ethers (the native cryptocurrency on the Ethereum blockchain), equivalent to US$290,000 at the time.[2] Another ground-breaking initiative was the sale by Christies of Beeple's *EVERYDAYS: THE FIRST 5000 DAYS* digital art piece in the

1 Tom Bateman, "Sorare football NFT game raises €580 million in record-breaking fundraising round - but what is it?" (*Euronews*, 21 September 2021) <https://www.euronews.com/next/2021/09/21/sorare-football-nft-game-raises-580-million-in-record-breaking-fundraising-round-but-what->.

2 Remi Lou, "Sorare : le NFT de Cristiano Ronaldo vendu presque 300 000 dollars" (*Journal du Geek*, 15 March 2021) <https://www.journaldugeek.com/2021/03/15/sorare-le-nft-de-cristiano-ronaldo-vendu-presque-300-000-dollars/>.

© EMERIC PRÉVOST, 2023 | DOI:10.1163/9789004514850_012
This is an open access chapter distributed under the terms of the CC BY-NC-ND 4.0 license.

form of an NFT for slightly more than US$69 million.[3] In the same vein, 9 NFTs attached to 9 unique items of a new (very fashionable) collection of Dolce & Gabbana recently sold for a total of US$5.65 million on the UNXD marketplace that leverages on the Polygon blockchain.[4]

Tokenisation is however not limited to digital art or online gaming and collectibles. Real estate is generally viewed as a prime sector where tokenisation is expected to thrive. One example is the *RealT* platform, managed by the Delaware company *RealToken*, which aims to enable investors world-wide to invest in the US real estate market through tokenised fractional ownership. As expressly mentioned on its Website and in its Terms of Service, *RealT* tokens issued on the Ethereum blockchain represent a fraction of ownership interest in a Limited Liability Company (LLC) owning and specifically dedicated to managing each specific real property.[5] This means in practice that such tokens give rights to a share of rental payments and possibly to voting rights on management decisions in relation to the property.[6] The sale of *RealT* tokens therefore clearly amounts to a private placement of securities under US law.[7]

On the other side of the Atlantic, the UK-based *Smartlands* platform is another good example of how real estate tokenisation is at present structured. *Smartlands* tokenises shares in real estate assets and issues Smartlands tokens (SLTs) on the Stellar blockchain.[8] In September 2018, the platform managed to close a record high private placement of security tokens in the UK, raising funds to buy 30% of beneficial interest in the shares of the private company owning a student housing block in Nottingham (UK).[9] Despite apparent disclaimers on

3 See at "Beeple's opus: Created over 5,000 days by the groundbreaking artist, this monumental collage was the first purely digital artwork (NFT) ever offered at Christie's" (*Christie's*) <https://www.christies.com/features/Monumental-collage-by-Beeple-is-first-purely-digital-artwork-NFT-to-come-to-auction-11510-7.aspx> accessed 29 June 2023.

4 See UNXD, "Upcoming Drops" (*UNXD*) <https://unxd.com/drops> accessed 30 September 2021. See also Ledger Insights, "Dolce & Gabbana sells 9 NFTs for $5.65 million" (*Ledger Insights*, 1 October 2021) <https://www.ledgerinsights.com/dolce-gabbana-sells-9-nfts-for-5-65-million/>.

5 RealT, "Fractional and frictionless real estate investing" (*RealT*) https://realt.co/ accessed 29 June 2023.

6 *Id.*

7 RealT, "Terms of Service" (*RealT*, 25 April 2019) <https://realt.co/terms-and-conditions/> (referring expressly to the security and speculative nature of ReatT tokens).

8 Definder, "News" (*Definder*) <https://smartlands.io/news/> accessed 4 September 2021.

9 Definder, "Smartlands Successfully Closes Sale of Security Tokens in Student Accommodation Block in Nottingham, UK" (*Definder*, 28 August 2019) <https://smartlands.io/blog/smartlands-successfully-closes-sale-of-security-tokens-in-student-accommodation-block-in-nottingham-uk/>.

its website that *Smartlands* does not provide investment services, consultation of the public register of the UK Financial Conduct Authority (FCA) shows that *Smartlands Platform Ltd* was previously an appointed representative of the FCA licensed firm *Shojin Financial Services Ltd*, up until it acquired the latter in 2019 to get the direct benefit of the license allowing for the management of a small UK authorised alternative investment fund.[10] *Smartlands* tokens would thus qualify as units in a collective investment scheme with the effect of triggering the application of securities regulation. Although asset tokenisation leverages on DLT, it resembles asset-backed securitisation in many ways. Acknowledging such a feature is essential to address the conflict-of-laws issues raised by asset tokenisation.

Another question however is that of the use of DLTs and blockchains by public authorities to enhance the efficiency of land registers. The "digital street" project of the UK HM Land Register that intends to leverage on the Corda DLT is one among other initiatives.[11] Real estate tokenisation is indeed a multiple dimensions process that involves steps, including consultation of the public land registry, conclusion of a sale agreement, conclusion of a mortgage agreement by the buyer, *etc*.[12] Besides real estate, moveable assets such as vehicles may also be tokenised.[13] The core legal question however remains: what right in the underlying asset (ownership right, right to use, *etc*.) is granted to the token holder and according to which applicable law the content of such right(s) shall be determined?

The above examples set the stage for a legal analysis of the digital representation of assets in the form of tokens. Bearing in mind the above case scenarios, it should be recalled that the primary purpose of asset tokenisation is about asset monetisation and increasing the liquidity of otherwise poorly liquid assets. It is thus paramount to briefly ponder how DLTs and blockchains allow for such asset tokenisation. The blockchain as such first emerged as a peer-to-peer electronic cash system, where a "coin" is a chain of digital signatures enabling the transfer of data bytes from one person to the other thanks to a set of private and public cryptographic keys (in practice simply a sequence

10 Financial Conduct Authority, "FCA Public Register" (*FCA*) <https://register.fca.org.uk/s/search?q=smartlands&type=Companies> accessed 29 June 2023.

11 Gareth Robson, "Enhancing our registers" (*HM Land Registry*, 1 October 2019) <https://hmlandregistry.blog.gov.uk/2019/10/01/enhancing-our-registers/#comments>.

12 UCL CBT, HM Land Registry, and Mishcon de Reya LLP, "UCL CBT DLT in Land Registry White Paper" (*UCL*, 6 March 2019) <http://blockchain.cs.ucl.ac.uk/dlt-land-registry-white-paper/>.

13 Bitcars, "Home" (*Bitcars*) <https://bitcars.eu/#> accessed 29 June 2023.

of numbers and letters).[14] Transactions (or any kind of information) are periodically and at a fixed frequency registered in digital blocks of a determined amount of megabytes after their validation by one or more validating (or "mining") nodes. Each validating or controlling node of the network keeps a copy of all or part of the chain of blocks on their servers (or servers to which they have access). Information is therefore stored in multiple unknown locations (at least in an open and fully distributed model). Once a transaction or information is registered in a block, there is no way back. It is virtually impossible to alter such a register, except if the majority of the validating nodes agrees to it. Such an agreement is however deemed almost impossible to achieve in a fully distributed and anonymous network.[15] Blockchain or DLT-driven ecosystems can be open (or permissionless, *i.e.* allowing anyone to enter the network as participant) or closed (permissioned, *i.e.* where entry into the network is restricted), but are in any case characterised by their distributed, immutable and pseudonymous/anonymous nature. Such characteristics strongly reduce the role of intermediaries or even make them dispensable; this explains why the blockchain and DLTs are seen as disruptive of traditionally intermediated relations.[16] It is even more so with the development of smart contracts that allow for the automated performance of an agreement at predetermined conditions. Smart contracts can find many different applications, in particular in the context of Initial Coins Offerings (ICOs), as well as most recently, in the context of NFTs issuances. Remarkably, it is thanks to the development of smart contracts on the Ethereum blockchain and similar blockchains that various kinds of items have started to be encoded in the form of tokens.

The phenomenon of "tokenisation" is thus generally meant to refer to the representation of a right in the form of a digital asset dubbed "token" or "coloured coin."[17] This is technologically possible on DLTs or blockchains

14 Satoshi Nakamoto, "Bitcoin: A peer-to-peer Electronic Cash System" (*Bitcoin*, 24 May 2009), 2 <https://bitcoin.org/bitcoin.pdf>.

15 It has happened only a few times, and most famously to retrieve stolen tokens when the DAO (standing for "Decentralised Autonomous Organisation") project on the Ethereum protocol was hacked in 2016.

16 For further details on the definition and functioning of the blockchain and DLTs, please refer to: Jean Bacon et al., "Blockchain Demystified (Queen Mary School of Law Legal Studies Research Paper No. 268/2017)" (*SSRN*, 21 December 2017) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3091218>.

17 Olivier Hari and Ulysse Pasquier, "Blockchain and Distributed Ledger Technology (DLT): Academic Overview of the Technical and Legal Framework and Challenges for Lawyers" (2018) 5 International Business Law Journal 423, 423–447 (also distinguishing cryptocurrencies from tokens on the point that only tokens enshrine a specific right of a blockchain participant, which may include claims, right to payments or ownership rights).

thanks to smart contracts.[18] Parties can resort to different technological standards to design the core characteristics of a token. A token may be fungible, non-fungible or even non-transferable.[19] By metonymy (and somewhat abusively), the digital representation of full ownership rights is often referred to as the digital representation of assets, whether such assets are real (physical) assets (or "exogenous" assets) or traditional asset classes issued in tokenised form (*i.e.* "native" or "endogenous" assets).[20] A token is therefore two faced as it is both an asset in and by itself and a vehicle for the representation of rights in an underlying asset. The "Digital Assets and Private Law" project of the International Institute for the Unification of Private Law (UNIDROIT) interestingly labelled such tokens embodying, representing or linked to off-chain assets as "digital twins," that would include NFTs, tokens backed by off-chain assets, tokens backed by digital assets, and decentralised finance (DeFi) assets.[21]

The question of the law applicable to the determination of proprietary rights conveyed by digital twins in the underlying asset is two-fold: on the one hand, the law applicable to the right of the token holder in the token itself, and on the other hand, the law applicable to the right of the token holder in the underlying asset. The respective connecting factors may differ and lead to different applicable laws. Discrepancies of conflict-of-laws rules may therefore result in substantial law divergences between the title attached to tokens and proprietary rights in the underlying asset. To some extent, the cyber and the physical dimensions of the world of things need to be reconciled.[22] We shall refer to such conflict situation as intra-systemic: it is for each single legal system to resolve internally the risk of divergence between the law applicable at the underlying level and the law applicable at the token level. The approach may be dual, if two conflict-of-laws rules co-exist, or unitary, if there is one

18 Rosa M. Garcia-Teruel and Héctor Simón-Moreno, "The digital tokenization of property rights. A comparative perspective" (2021) 41 Computer Law & Security Review 1, 2.

19 *Id.* (noting that on Ethereum the ERC-20 protocol enables the creation of fungible tokens, whereas the ERC-721 protocol allows for the creation of non-fungible tokens and the ERC-1238 protocol permits creating non-transferable tokens).

20 OECD, "Regulatory Approaches to the Tokenisation of Assets" (*OECD*, 26 January 2021), 10 <www.oecd.org/finance/Regulatory-Approaches-to-the-Tokenisation-of-Assets.htm>.

21 UNIDROIT, "Digital Assets and Private Law (Study LXXXII, W.G.3, Doc. 2 (rev. 1))" (*UNIDROIT*, June 2021) <https://www.unidroit.org/work-in-progress/digital-assets-and-private-law/> accessed 5 June 2022.

22 Florian Möslein, "Conflicts of Laws and Codes. Defining the Boundaries of Digital Jurisdictions," in Philipp Hacker et al. (eds), *Regulating Blockchain: Techno-Social and Legal* (Oxford: OUP 2019), 275–288 (distinguishing between conflict situations of the technology and the law to be dealt with domestically on one hand and the coordination of legal systems through conflict-of-laws rules as long as nation states exist on the other hand).

single conflict-of-laws rule for issues related to both the token and the underlying asset. Following a unitary approach, either the law applicable to the underlying asset or the one applicable to the token shall prevail and govern both dimensions. Various solutions are possible and ultimately depend on policy choices within each system of law. Nevertheless, the way each legal system deals with intra-systemic conflicts entails inter-systemic consequences.[23] A unitary intra-systemic approach favouring the connection and applicable law of the underlying asset would be allegedly compatible with a bilateral conflict-of-laws rule. On the contrary, a unitary approach favouring the law applicable to tokens would at first sight require a unilateral conflict-of-laws rule given the ubiquitous nature of tokens. In turn, a dual approach would trigger the need for reconciliation between the two co-existing conflict-of-laws rules that are likely to follow different methodologies. The present contribution therefore aims to analyse both the intra-systemic and inter-systemic conflict-of-laws issues arising from asset tokenisation. However, the issues relating to value-referenced tokens (*i.e.* stablecoins) will not be considered. A dedicated chapter will analyse the legal intricacies of stablecoins or so-called "asset-referenced tokens."[24,25] The specific issue of Central Bank Digital Currencies (CBDCs) will not be dealt with here either.[26] This being observed, the concept of "asset" will be used in a broad sense and will encompass *inter alia* tangibles and intangibles, registered and unregistered assets, moveables and immoveables, consumables and non-consumables. Various conflict-of-laws rules may therefore need to be combined.

23 Bernard Audit and Louis d'Avout, *Droit International Privé* (Paris: LGDJ 2018), para. 328 et seq., 284 et seq. (detailing private international law tools to deal with situations of conflict of systems of law).

24 See Article 3(1)(3) of the Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, [2020] COM/2020/593 final, 2020/0265(COD) ("MiCA") (defining "asset-referenced tokens" as "a type of crypto-asset that purports to maintain a stable value by referring to the value of several fiat currencies that are legal tender, one or several commodities or one or several crypto-assets, or a combination of such assets," and distinguishing from "electronic money tokens" defined in Article 3(1)(4) of the same regulation proposal as tokens meant "to be used as a means of exchange and that purports to maintain a stable value by referring to the value of a fiat currency that is legal tender").

25 See Chapter 13 by Matthias Lehmann and Hannes Meyle in this book.

26 See Chapter 12 by Caroline Kleiner in this book.

2 Asset Tokenisation at Risk of Legal Fragmentation

Despite all the trust one can have in the technology, it is at the end only through the law that a "tokenised economy" can truly come to light. There is little doubt that most, if not all, states will take part in the race to offer the most attractive legal and regulatory framework for the development of DLTs. The race has already started. This is manifest if attention is paid to the number of drafts or already enacted laws.[27] If a state were to abstain from introducing clear regulatory and private law rules for DLT ecosystems, transaction and opportunity costs for economic actors doing business in that state would rise. This is likely to put a state's market at a detrimental competitive disadvantage. This competition game is both the result and the cause of further inter-systemic legal fragmentation. At the intra-systemic level, however, if the concept of "tokenisation" is to be meaningful, *i.e.* if it is to correspond to a certain reality, legal systems should ensure that the holding and transfer of tokens equates the transfer of title to the rights in the underlying. In other words, substantial legal provisions should ensure that transfer of rights and their acquisition on DLT networks are valid and effective.[28]

Affording legal recognition to transactions over tokenised assets also implies that proprietary rights at both the token layer and the underlying layer must always coincide. Priority issues may indeed arise if title to a token with ownership rights in the underlying is transferred to person A, while at the same time ownership of the underlying asset is passed on to person B. Whose title of A or B has priority? Other issues that legal systems must cope with internally include for instance: the requirements for the perfection of transfers of title via tokens; the conditions for the creation of security interests over tokenised assets; the regime of encumbrances affecting digital twins and their underlying assets; the conditions and consequences of good faith acquisition of tokenised assets; the fate of tokenised assets in insolvency proceedings; *etc*. The dual existence of tokenised assets engenders glaring difficulties to provide a unitary answer to such proprietary issues. Difficulties stem from the distinctive legal nature of tokens and their underlying assets.

27 See for a brief overview of some already existing legislative acts: Hague Conference on Private International Law, "Developments with respect to PIL implications of the digital economy including DLT (Prel. Doc. No 4 of November 2020" (*HCCH*, March 2021), Annex II <https://assets.hcch.net/docs/8bdc7071-c324-4660-96bc-86efba6214f2.pdf> accessed 5 June 2022.

28 UNIDROIT (n 21).

3 Tokens as Financial Intangible *Res*

It should be recalled that the concept of tokenised assets fundamentally refers to the situation where rights in an asset (tangible or intangible, moveable or immoveable, fungible or non-fungible, consumable or non-consumable, *etc.*) are represented in the form of tokens thanks to smart contract applications on DLT networks. Tokens are unique pieces of computerised data, subject to the exclusive control of one or several persons holding the private cryptographic key. Tokens can thus *per se* be conceived as intangible assets, which can be either fungible or non-fungible, and consumable[29] or non-consumable, depending on their design.[30] In other words, tokens may qualify as *res*.

Such qualification is, however, at first sight, at least, at odds with the fact that DLTs are generally considered as mere technological tools to which the law should remain neutral. In that sense, tokens may ultimately be considered as simple vehicles for the registration, representation and recording of transactions. At the end of the day, DLTs may simply amount to a mere process of digital registration of assets and transactions. If that were the intra-systemic approach taken, fundamental proprietary issues would remain governed by existing conflict-of-laws rules without much need of further changes. At best, it could be argued that the classic *lex situs* rule should be distinguished from the *lex registrationis*, the latter governing simply the conditions and processes of registration.[31] Connecting factors such as the elective *situs* (where an express choice of law governing the ledger is made) or the place of habitual residence or establishment of the administrator of the ledger would be particularly

29 A token may qualify as a "consumable" thing only insofar as it ceases to "exist" upon its first utilisation. Money is thus generally characterised as a consumable thing. The consumable nature of tokens however ultimately depends on their inherent characteristics. On this point, see among others: Axel Anderl, Markus Aigner, and Dominik Schelling, "Zivilrechtliche Aspekte," in Axel Anderl (ed), *Blockchain in der Rechtspraxis* (Wien: LexisNexis 2020), 59–60 (distinguishing between "coins," such as ethers, bitcoins, *etc.*, which are consumables akin to money, and security tokens, which are not); Dominique Légeais, *Blockchain et actifs numériques* (Paris: LexisNexis 2021), 218 (noting that tokens are intangibles, moveables, and consumables akin to money). Xavier Vamparys, *La Blockchain au service de la finance. Cadre juridique et applications pratiques* (Paris: Revue Banque 2018), 102 (noting that utility tokens may qualify as consumables, whereas "traceability tokens" may not); Louis Soleranski, "Réflexions sur la nature juridique des tokens" (2018) 3 Bulletin Joly Bourse, pt. 10 (noting that tokens should generally not qualify as consumables, except if they can be disposed of similarly to money).

30 Anderl, Aigner, and Schelling (n 29), 59–64.

31 Sjef van Erp, "Lex rei sitae: The Territorial Side of Classical Property Law," in Christine Godt (ed), *Regulatory Property Rights: The Transforming Notion of Property in Transnational Business Regulation* (Leiden: Brill | Nijhoff 2016).

relevant for such distinctive *lex registrationis* rules.[32] Other more intricate issues would however arise if DLTs are recognised intra-systematically as title transfer mechanisms, as legal systems would need to ensure both intra and inter systemic coherence between the title to the token and the title to the underlying assets. The distinction between "DLT record ledgers" and "DLT title ledgers" is therefore paramount, including for conflict-of-laws analysis.[33]

With this in mind, some core conditions would have to be met for DLT title ledgers to emerge and operate effectively. It should first be admitted intra-systemically that legal rights may constitute as such pieces of property to which property rights attach.[34] Second, DLTs should be recognised (albeit upon certain conditions being met) as valid transfer mechanisms (and not simply as an evidentiary system). However, even if DLTs are recognised as valid transfer mechanisms, the question remains as to whether the right derived from holding a token is a mere entitlement (or obligatory claim) over a right in the underlying asset, or a direct property right to the right in the underlying asset. Both paths are possible, but acknowledging a direct property right is the stronger option to unwind the full potential of disintermediated transactions through DTLs. Instead, recognising the holding of tokens as an entitlement to a right would require sticking to intermediated network architectures where it is always possible to identify the relevant intermediary against whom a corresponding claim may be lodged. If, however, the direct property right option is retained, intermediaries may still exist, but their role will be limited (*e.g.* they may act as simple custodians). To give a real and maximal legal effect to the tokenisation of assets, it is therefore argued that tokens should be granted legal existence as *res*. This is also the position taken in many jurisdictions which have passed specific laws on the matter.[35]

---

32 For further details and discussion on such candidate connecting factors, see developments *infra* in section 5 et seq.

33 Financial Market Law Committee (FMLC), "Distributed Ledger Technology and Governing Law: Issues of Legal Uncertainty" (*FMLC*, March 2018), margin no. 3.4 <http://fmlc.org/wp-content/uploads/2018/05/dlt_paper.pdf> accessed 5 June 2022.

34 James Y. Stern, "Property's Constitution" (2013) 101 California Law Review 277, 303 with the references cited (arguing that a right can be conceived as a "thing" and that a right is ultimately "a legal relationship—an entitlement—over which the holder has title").

35 Article L.552-2 of the French *Code monétaire et financier* (setting out that a token (*jeton*) is an "intangible asset representing, in digital form, one or more rights that can be issued, recorded, stored or transferred by means of a shared electronic recording device making it possible to identify, directly or indirectly, the owner of said asset" (translation by the author)). Article 2(1)(c) of the Liechtenstein Law of 3 October 2019 on Tokens and Trustworthy Technology (TT) Service Providers ("TVTG" or also hereinafter "Liechtenstein Blockchain Law") (referring to "pieces of information" clearly assigned, which,

Considering tokens as *res* bears several consequences. First, it acknowledges the transmutation of off-chain assets, as assets will be endowed with tokens' features, thereby easing their transfer, trade and management transnationally. The advantages of asset tokenisation are various. Alongside the possibility to turn illiquid assets into liquid ones that can then more easily be traded on a secondary market and across borders, tokenisation also allows for the reduction of transaction costs and risks thanks to fewer intermediaries and the trustworthy immutability of DLTs.[36] Tokenisation fundamentally widens financing options by lowering investment thresholds and broadening the range of potential investors (including foreign and non-professional investors). The monetisation function of tokenisation would however require an acknowledgement that tokens constitute a specific kind of financial asset with intrinsic credit, liquidity, operational and market risks. This will lead to link inevitably private law concepts to public law considerations and securities law characterisations. Whether or not tokens are negotiable and tradable financial assets impacts on private law conditions for the transfer, acquisition, redemption, *etc*. of tokens.

Tokenisation of off-chain assets for monetisation purposes thus ultimately questions the generally shared tripartite distinction between utility tokens (which enshrine rights to future services or products of the issuer), investment or security tokens (representing financial and membership rights), and currency or payment tokens such as bitcoins, ethers, *etc.* as media of exchanges.[37] The categorisation of tokens is important *prima facie,* as it leads to different legal and regulatory treatments. Such categorisation is however not as clear-cut as it may first seem. The generally less regulated utility tokens may indeed

---

when recorded on a DLT system such as the blockchain, "can represent claims or rights of memberships against a person, rights to property or other absolute or relative rights"). In Wyoming, United States, see section 34-29-101 of the WS introduced by the 2019 WS Digital Assets Existing Law no. SF0125 (distinguishing three mutually exclusive categories of digital assets, namely "digital consumer assets," "digital securities," and "virtual currencies," and characterising *de jure* tokens as "intangible personal property"). It is worth noting, however, that the 2018 US Supplemental Commercial Law for the Uniform Regulation of Virtual Currency Businesses Act, which amends Article 8 of the Uniform Commercial Code (UCC), recognises only an obligatory right (entitlement) to the holder of virtual currencies.

36 See, focusing on real estate, Josh D. Morton, "Blockchain Holds Potential For Commercial Real Estate" (*Law360*, 4 January 2021) <https://www.law360.com/articles/1339569/blockchain-holds-potential-for-commercial-real-estate>. See also more generally: Clément Jeanneau, "L'âge du Web décentralisé" (*Digital New Deal Foundation*, April 2018) <https://www.thedigitalnewdeal.org/wp-content/uploads/2017/06/the_digital_new_deal-org-JEANNEAU-Clement-LAgeDuWebDecentralise.pdf> accessed 5 June 2022.

37 Vamparys (n 29), 95 et seq.

be requalified as payment or security tokens, as the case may be, depending on their specific design and characteristics;[38] this represents a significant risk for users and intermediaries in terms of legal certainty and security. The uncertainty of such a tripartite categorisation has led to calls for clarification at the European level.[39] The European proposal for a MiCA Regulation[40] and a PILOT Regime Regulation[41] do not however solve the issue, as they take a similar approach by distinguishing between crypto assets (sub-divided into asset-referenced tokens, e-money tokens and utility tokens) and securities tokens.[42] Some jurisdictions have however attempted to bridge the gap by either allowing parties to a transaction to expressly characterise a token as a financial asset (*e.g.* Wyoming in the United States)[43] or by directly subjecting a wide range of tokens and virtual assets to the legal regime applicable to financial assets.[44] Characterising tokens as financial assets raises, however, other difficulties, as it would trigger the application of securities regulations which contain choice-of-law rules specifically adapted to the intermediated securities holding system.[45] This difficulty will be further detailed below.[46]

38 Thierry Bonneau et al., *Droit Financier* (3rd edn, Paris: LGDJ 2021), no. 842 at 539–543 (stressing that the qualification of financial instruments, such as shares or bonds, does not necessarily depend on the "monetary" nature of the return on the initial investment, since said return may at times also be in kind, *e.g.*, in the form of shares, products, or services, thus potentially bringing *prima facie* "utility tokens" within the scope of securities regulations).

39 Haut Comité Juridique de la Place de Paris (HCJP), "Les titres financiers digitaux «Security Tokens»" (*HCJP*, 27 November 2020), 9 <https://www.hcjp.fr/marches-financiers>.

40 MiCA (n 24).

41 Regulation (EU) 2022/858 of the European Parliament and of the Council of 30 May 2022 on a pilot regime for market infrastructures based on distributed ledger technology.

42 Article 2 (excluding tokens qualifying as securities) and Article 3 (setting out the definitions of crypto-asset categories) of the MiCA (n 24).

43 Section 34-29-101 of the WS introduced by 2019 WS Digital Assets Existing Law (n 35).

44 Uniform Law Commission's 2017 Uniform Regulation of Virtual-Currency Businesses Act (URVCBA) (Defining broadly the notion of "virtual currencies" to encompass both utility and investment types of tokens, which are considered "financial assets" for regulatory purposes given their "transferability" and "convertibility").

45 See for instance the 2018 Supplemental Commercial Law for the Uniform Regulation of Virtual Currency Businesses Act, which amends Article 8 of the Uniform Commercial Code (UCC) and makes direct references to the Hague Convention of 5 July 2006 on the Law Applicable to Certain Rights in Respect of Securities Held with an Intermediary (The Hague Securities Convention).

46 See *infra* section 6.

This being observed, analogies have been drawn between tokens representing rights in off-chain assets and commercial papers.[47] The case made is that tokens may qualify as digital documents of title or negotiable instruments, provided that specific legal provisions are passed to that effect.[48] Stemming from English law, the notion of "negotiable instrument" is to be understood as "an instrument that contains a promise of payment" (not necessarily a monetary payment), thereby constituting per se a "store of value" which can be passed on "free of any defects" without the need for the transferee to check legal title.[49] The negotiable nature of financial instruments is however also generally acknowledged under legal systems other than the English legal system. French law for instance contains specific provisions on the negotiable character of financial instruments and its legal consequences.[50] The German law concept of "Wertpapier" is similar,[51] and has recently been adapted to suit the development of DLTs.[52] Characterising tokens as negotiable instruments would thus acknowledge their financial nature, and would prompt legal systems to subject tokens to suitable civil law regimes, involving notably good faith acquisition principles. Liechtenstein[53] is a good example of a state having introduced specific provisions governing notably the right of disposal, the disposal and transfer processes, and the principle of good faith acquisition of tokens.[54] Another example is the Swiss DLT Act that entered into force on 1st February 2021, and significantly amended Swiss private and private international law.[55]

Second, considering tokens as *res* also implies that proprietary rights attach to the tokens themselves and not directly to the underlying rights. The question of whether the underlying rights are *in rem* or *in personam* would therefore not

47 UNIDROIT (n 21), margin no. 86 (noting that "commercial paper embodies a right in such a manner that holding the document is equated to holding the right").

48 *Id*., margin nos. 86 and 92.

49 Alfonso-Luis Calvo Caravaca and Javier Carrascosa González, "Chapter 1: Scope," in Ulrich Magnus and Peter Mankowski (eds), *Rome I Regulation – Commentary* (Köln: Verlag Dr. Otto Schmidt 2017), vol. 2, 52 et seq., margin no. 9.

50 Articles L.211-14 to L.211-16 of the French *Code monétaire et financier* (n 35).

51 Wertpapierhandelsgesetz (WpHG), Abs 1§2.

52 Gesetz über elektronische Wertpapiere vom 3. Juni 2021 (BGBL. I S. 1423) («eWpG»); see in particular the definition of electronic transferable securities in Abschnitt 1 §2 Elektronisches Wertpapier.

53 Liechtenstein Blockchain Law (n 35).

54 *Id*., Articles 5 to 9.

55 Swiss Federal Act of 25 September 2020 on the Adaptation of Federal Law to Developments in Distributed Electronic Ledger Technology, FF 2020 7559. For an overview of the amendments made to the Swiss Code of Obligations, see Tarek Houdrouge and Jérémie Tenot, «Registres électroniques distribues: de l'ombre à la lumière-le cas de la Suisse» (2021) Revue de droit des affaires internationales 227.

matter as such. Rights over tokens would however qualify as a kind of right *in rem* that legal systems would need to recognise to secure the validity and legal effect of disposal and acquisition of tokens.[56] It is worth noting that this view is fully in line with the right to the protection of property enshrined at Article 1 Protocol 1 of the European Convention on Human Rights (CEDH), which encompasses the protection of any "possession," including claims, intangible assets, intellectual property, irrespectively of whether the rights are *in rem* or *in personam* under domestic law.[57] In this context, some have advocated for a cosmopolitan analysis of property rights based on a functional approach in order to overcome the dogmatic limitations of domestic property law regimes and to better suit virtual assets.[58] In practice, courts of several jurisdictions have already enforced property rights to the benefit of holders of crypto assets, even in the case of cryptocurrencies such as bitcoin and ether which are not backed by any asset.[59]

At first sight, property law would indeed be particularly relevant as it aims to allocate the legal authority (or title) to determine and control the use of a *res* subject to rivalry.[60] While tokenisation allows for increased liquidity through the fractioning of rights, it also enables the creation of rivalry (*i.e.* making a thing the object of competing interests). The phenomenon of NFTs is a brilliant illustration thereof. By ensuring the uniqueness of images, Gifs, memes, card games, audio-visual art pieces and the like, NFTs ensure both

56 Stern (n 34), 304 (arguing that property rights can attach to any kind of right and that "the creation of an *in personam* right entails the creation of an additional right *in rem*, the *res* being the underlying *in personam* right"). Also, see Hubert de Vauplane, "Blockchain and Intermediated Securities" (2018) 1 National Insurance Producer Registry (discussing matters of securities registered on a blockchain, whether the "fiction" of rights *in rem* is still relevant, and asking the question of whether a "new form of right in rem on digital assets" should be introduced to better reflect technological realities). Shawn Bayern, "Dynamic Common Law and Technological Change: The Classification of Bitcoin" (2014) 71 Washington and Lee Law Review Online 22 (advocating for a reconceptualisation of property rights for cryptocurrencies such as bitcoin).

57 European Court of Human Rights, "Guide on Article 1 of Protocol No. 1 to the European Convention on Human Rights" (Council of Europe, 31 December 2021), <https://www.echr.coe.int/Documents/Guide_Art_1_Protocol_1_ENG.pdf>.

58 Caterina Sganga, "Cracking the Citadel Walls: A Functional Approach to Cosmopolitan Property Models within and Beyond National Property Regimes" (2014) 3 Cambridge Journal of International and Comparative Law 770.

59 For a presentation of various cases and their analysis, see Chiara Zilioli, "Crypto-Assets: Legal Characterisation and Challenges under Private Law" (2020) 45 European Law Review 251.

60 James Y. Stern, "Property, Exclusivity, and Jurisdiction" (2014) 100 Virginia Law Review 111; Stern (n 34).

scarcity and rivalry, thereby making them valuable and tradeable assets. Tokens appear to fulfil both conditions of a *res*: they are specific enough (as they are represented by unique and identifiable encoded data) and they are "good-against-the-world" (*i.e.* enforceable against third parties, in particular when issued on public blockchains such as Ethereum).[61] Rules of property law in a tokenised economy would thus fundamentally pursue the same classical role of allocation of rights as a zero-sum game, meaning that one person's rights over a token is exclusive and necessarily comes at the expense of any other person. The exclusivity of property rights attached to tokens is ensured by the technical feature of blockchains preventing double spending issues (meaning that only the transaction entered first will ultimately go through).[62] However, given the inherent cross-border nature of blockchains and DLTs,[63] conflict-of-laws issues inevitably arise in a world where private property law regimes are fragmented. Although comparative law analysis has generally concluded that transfer of property rights may be conducted via tokens under various private law regimes, substantive legal requirements still vary depending on the applicable law.[64] Ongoing projects such as the UNIDROIT "Digital Assets and Private Law" project[65] for the harmonisation of substantive private law regimes applicable to tokens and other digital assets will help prevent unbearable discrepancies, but are not likely to suppress the need for coordination through conflict-of-laws rules.

4 Conflict-of-Laws Implications

4.1 *Connecting the Underlying Assets*

Considering tokens as financial intangible *res* raises many questions as to the relevant conflict-of-laws rule at the token layer and its coordination with the

61 Stern (n 60), "Property, Exclusivity, and Jurisdiction."

62 Nakamoto (n 14) (double spending issues being resolved on the original Bitcoin blockchain by the public validation and timestamping of transactions' blocks according to the proof-of-work consensus mechanism).

63 Florence Guillaume, "*Blockchain* : le pont du droit international privé entre l'espace numérique et l'espace physique," in Ilaria Pretelli (ed), *Conflict of Laws in the Maze of Digital* (Genève/Zurich: Schulthess Éditions Romandes 2018), 164–188 (arguing that the internationality or cross-border nature of transactions conducted on blockchains can be assumed).

64 Garcia-Teruel and Simón-Moreno (n 18), 41 (distinguishing the transfer of property rights via tokens in jurisdictions adopting a "consensual system," a "title and modus system," or an "abstract problem," and concluding that metadata of smart contracts may be made legally compliant whatever the applicable system).

65 UNIDROIT (n 21).

law applicable at the underlying level. It has been noted that the law applicable to the underlying assets would generally be determined according to the normally applicable conflict rule: *lex rei sitae* for tangible moveables and immoveables; *lex protectionis* for intellectual property rights; *lex societatis*; *etc*.[66] Arguably, courts would apply the same conflicts rule at the token level.[67] The rationale for such a view is that the change introduced by DLTs and tokenisation is merely technological.[68] Such a view contrasts, however, with the consideration that tokens are financial intangible *res*. The underpinning risk is to undermine the main advantages of asset tokenisation (*i.e.* liquidity and reduced transaction costs). Favouring the law applicable to the underlying asset would also result in a legal fragmentation of DLT ecosystems, since the proprietary effect of transactions on such networks will ultimately depend on a wide variety of laws.

In case of the token representation of tangible moveables, the law applicable to the transfer of title may also shift over time depending on the geographical location of the underlying. Such shift may cause daunting issues if the power and time of disposal of tokens is dealt with differently across jurisdictions and the underlying tangible moveable has been moved from one jurisdiction to another. Let's posit that jurisdiction X authorises transfer of ownership rights in tangible moveables via tokens and has a set of specific legal provisions to that effect. Person A mints (*i.e.* creates) a token while the good is in jurisdiction X. The transfer of ownership rights via the sale of the token by person A to person B will be governed by the law of jurisdiction X as the *lex situs*. If the token is burnt (*i.e.* sent to an unusable wallet) immediately following a request of redemption by B to take possession of the good, the story ends. However, difficulties arise if B immediately transfers the token to C, whereas, in the meantime, the good has been moved to another jurisdiction Y, where the transfer of tangible moveables via tokens is not legally possible. Applying the law of Y as the *lex situs* for the transaction between B and C would lead to the conclusion that C has not acquired good title in the underlying. In such case, C will be left only with a contractual claim against B. This situation is at odds with the economy of a transaction over tokenised assets where the holding of a token purports to establish a direct relationship with the token issuer. Such a case scenario should not however suggest that the *lex situs* is irrelevant as a matter

66 *Id*., 56. See also FMLC (n 33), margin no. 4.8 (opining that where DLT transactions aim to dispose of the title in an underlying tangible asset, it is unlikely that courts will depart from the *lex situs* of the underlying asset).

67 HCCH (n 27) (noting that tokens representing tangible property are most likely to be held subject to the *lex situs* of the underlying asset). See also UNIDROIT (n 21), 56.

68 *Id*.

of principle; it simply shows that intricate issues may arise if a *prima facie* preference is given to the *lex situs*. A possible legal solution that is arguably better suited to the needs and purpose of asset tokenisation will be detailed in section 4.4 below. A technical solution would be to restrict the onward sales of the same tokens, which would however impede the development of secondary markets and limit the benefits of asset tokenisation.

The straight application of the *lex situs* rule at the token level may furthermore increase the costs and restrict the possibility of using tokens as collateral to secure transactions. It is possible indeed that the *lex situs* of an underlying asset overrides and prevents the constitution and perfection of a collateral arrangement over a tokenised asset.[69] Secured transaction laws should therefore be amended to ensure that security rights constituted over negotiable tokens correspond to valid security rights over the underlying asset.[70] On the front of transfers of intellectual property rights such as copyrights via tokens, less problematic issues would arise, as the *lex protectionis* would arguably apply regardless of the chain of intermediaries or transactions. It is therefore argued that a bilateral conflict-of-laws rule whose connecting factor is the geographical location of the underlying asset may not fit the purposes of asset tokenisation.

4.2 *Connecting the DLT Network*

At the token level, finding the right connecting factor for a bilateral conflict-of-laws rule seems even more problematic. Several approaches may be contemplated.

One way would be to apply one single law to each DLT systems where tokens are issued and transferred. This would yield the benefit of certainty as one single law would apply to proprietary aspects of all transactions conducted on one given DLT system. It would also take due account of the financial nature of tokens and would be consonant with the system-centred approach advocated for intermediated securities.[71] In the absence of another choice of law by the parties to a transaction over tokenised assets, such unitary approach would also align the *lex contractus* with the law governing

69 UNIDROIT (n 21), margin no. 93 (noting that secured transactions laws based on the 2016 UNCITRAL Model Law on Secured Transactions would apply to tokenised assets, thereby allowing for their collateralisation, but without the certainty that a security right in the digital asset would also convey a security right in the underlying tangible asset).

70 *Id*., margin no. 96.

71 Maisie Ooi, "The Choice of a Choice of Law Rule," in Louise Gullifer and Jennifer Payne (eds), *Intermediated Securities: Legal Problems and Practical Issues* (Hart Publishing 2010), 117–127.

proprietary transfers.[72] Alignment of contractual and proprietary issues would be ensured by the simple accession to a DLT system (miners and users alike), similarly to the situation of market participants adhering to market infrastructures such as clearing houses.[73]

Yet, subjecting DLT systems to one single law is not free from difficulties. First, a proper connecting factor needs to be found. Attempts have been made to subject entire DLT ecosystems (*e.g.* the Bitcoin blockchain ecosystem) to one single state law by means of the proximity principle (*i.e.* applying the closest and most real connection test), and taking into account various criteria such as the place of residence of the initial developers, the source of funding, and the development license.[74] Under this approach, the Primary Residence of the original Coder (PResC) would appear to be a primary factor to take into account to designate the state law applicable to the code itself (*lex codicis* or *lex digitalis*). However, the code itself is only the technological infrastructure which supports variegated applications. The link of such *lex codicis* (assuming that it can be objectively determined) may rightfully appear rather tenuous, given the various practical applications of DLTs.[75]

Another connecting factor may be the elective *situs* (or chosen law), whereby participants to a DLT network freely choose the law governing proprietary issues.[76] This solution has been notably advocated by the International Swap Derivative Association (ISDA), whilst acknowledging the need for restricting the choice of DLT participants to ensure sound and adequate policy, legal and regulatory oversight.[77] In its response to the public consultation

72 See for instance Article 4(1)(h) of the Rome I Regulation (Regulation no 593/2008 of 17 June 2008 on the law applicable to contractual obligations (Rome I), [2008] OJ L177/6 ("Rome I Regulation")) which designates, in the absence of an express choice by the parties, the law of the relevant market or multilateral system as the *lex contractus* governing the transactions over instruments traded on such market.

73 FMLC (n 33), margin no. 6.7.

74 Michael Ng, "Choice of law for property issues regarding Bitcoin under English law" (2019) 15 Journal of Private International Law 315 (pointing out Massachusetts law as the law governing the Bitcoin blockchain ecosystem pursuant to English conflict of laws).

75 HCCH (n 27).

76 Note that the "elective situs" terminology is generally used to underline and preserve the analogy with the PRIMA+ conflict-of-law rule set out in the 2006 Hague Securities Convention (n 45) that allows parties to choose the law applicable to proprietary issues of intermediated securities; for further details, please refer to section 4.3 *infra*. FMLC (n 33), nos. 6.4 to 6.8 also preserve such an analogy in the context of DLTs.

77 ISDA et al., "Private International Law Aspects of Smart Derivatives Contracts Utilizing Distributed Ledger Technology" (*ISDA*, 13 January 2020) <https://www.isda.org/2020/01/13/private-international-law-aspects-of-smart-derivatives-contracts-utilizing-distributed-ledger-technology/>.

on the reform of the European Settlement Finality Directive (SFD)[78] and the European Financial Collateral Directive (FCD),[79] ISDA further pleaded for a cross-sectorial adoption of an elective *situs* rule at the international level.[80] The connecting factor would therefore be the elective *situs* rule within the limits set by the competent regulator.[81]

The issue shifts however to the determination of the competent regulator, which may be particularly difficult to establish if participants are located in different jurisdictions and if the regulatory framework is not harmonised. Elective *situs* or modified elective *situs* would also prove difficult in fully distributed and permissionless networks. Although examples show that the financial industry seeks to develop permissioned DLT platforms,[82] tests of securities token transactions on public and permissionless DLT networks such as Ethereum have already led to successful and positive results.[83] From an industry point-of-view, public and permissionless DLTs should provide even better liquidity gains than private and permissioned DLTs, thereby questioning the practical relevance of an elective *situs* criterion as a connecting factor in such cases. The elective *situs* criterion may also face opposition where legal systems

78 Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems, [1998] OJ L166/45 ("Settlement Finality Directive").

79 Directive 2002/47/EC of the European Parliament and of the Council of 6 June 2002 on financial collateral arrangements, [2002] OJ L168/43 ("Financial Collateral Directive").

80 Responses to the European Council, "Targeted consultation on the review of the Directive on settlement finality in payment and securities settlement systems" (*EC*) <https://ec.europa.eu/info/consultations/finance-2021-settlement-finality-review_en> accessed 10 October 2021. Also, Responses to the European Council, "Targeted consultation on the review of the Directive on financial collateral arrangements" (*EC*) <https://ec.europa.eu/info/consultations/finance-2021-financial-collateral-review_en> accessed 10 October 2021.

81 HCCH (n 27) (designating such connecting factor as "modified elective *situs*" and interestingly highlighting that the Hague Securities Convention similarly limits the freedom of parties to choose the law applicable to a securities account). FMLC (n 33), margin no. 6.9.

82 See, amongst others, the Liquidshare platform that leverages on permissioned and proprietary DLTs: Liquidshare, "Technology" (*Liquidshare*) <https://liquidshare.io/technology/> accessed 5 June 2022.

83 See for instance the issuance of 27 April 2021 of a digital bond by the European Investment Bank (EIB) in collaboration with Goldman Sachs, Santander and Société Générale: Société Générale, "European Investment Bank (EIB) Issues its First Ever Digital Bond on a Public Blockchain" (*SG Forge*, 27 April 2021) <https://www.sgforge.com/european-investment-bank-eib-issues-its-first-ever-digital-bond-on-a-public-blockchain/> and Société Générale, "Securities Finance Trade of a Digital Bond Issued on Public Blockchain Initiated by Societe Generale And SG-Forge" (*SG Forge*) <https://www.sgforge.com/securities-finance-trade-digital-bond-on-public-blockchain/> accessed 10 October 2021.

do not allow a subjective choice of law in matters of property law.[84] A "deemed elective *situs*" factor whereby the law of the DLT system is determined by the competent regulator(s) would not resolve the issue, as here again the issue will shift to one of territorially-limited regulatory law.[85]

As a fall-back rule, however, if no choice of law has been made by the DLT participants, the Place of the Relevant Operating Authority or Administrator Approach (PROPA) has been envisaged.[86] Although PROPA would be an objective connecting factor, it would prove impracticable in fully distributed DLT networks, and *a fortiori* in networks whose governance follows the path of a Decentralised Autonomous Organisation (DAO). The same issues arise with the Private Encryption Master keyholder Approach (PREMA), where the focus is put on the DLT Administrator or other third-party that holds the master key granting ultimate control over DLT transactions.[87]

Today, many exchanges and platforms follow a decentralised structure and issue their own governance tokens.[88] This makes it particularly difficult to apply the above-mentioned PROPA or PREMA approaches. In addition, assets can be tokenised on different platforms which rely on the same or different blockchains or other DLT systems.[89] In the case of tokenised assets, however, the fundamental issue is to ensure that token transactions are reflected at the underlying layer. The risks reside at the enforcement stage. Opting for a DLT-system or DLT platform-centred approach would require legal systems to recognise that the law of DLT systems govern proprietary issues of transactions over tokenised assets. Market participants transacting over tokenised assets would also likely incur important costs as legal opinions would be necessary to ensure enforceability of their dealings.

84 FMLC (n 33), margin no. 6.7.

85 *Id*., margin no. 6.11. HCCH (n 27).

86 FMLC (n 33), margin nos. 6.16 and 6.17. HCCH (n 27).

87 FMLC (n 33), margin no. 6.18. HCCH (n 27).

88 Légeais (n 29), 169–170 (distinguishing between centralised, semi-centralised, and decentralised platforms). The Binance platform is, among others, a typical example of a decentralised platform which issues its own coin: the BNB; see Binance, "What is BNB?" (*Binance*) <https://www.binance.com/en/bnb> accessed 6 June 2022. However, Binance recently started to recentralise its operations for regulatory compliance purposes. Another example of a decentralised exchange with high trading volumes is Uniswap, which issues UNI coins; see Uniswap, "Uniswap Protocol" (*Uniswap*) <https://uniswap.org/> accessed 6 June 2022.

89 See amongst other the OpenSea platform, OpenSea, "Discover, collect, and sell extraordinary NFTs" <https://opensea.io/> accessed 6 June 2022, which allows for the minting of NFTs, either on Ethereum or on the Polygon blockchain compatible with Ethereum.

4.3 *Connecting the Token or the Token Wallet*

Another approach to craft a bilateral conflict-of-laws rule at the token level would be to focus on DLT products, *i.e.* the tokens themselves. If tokens qualify as a kind of negotiable instrument akin to commercial papers, the holding and exchange of tokens would entail the valid constitution and transfer of title over the underlying asset.

However, this material and intra-systemic characterisation would not solve the conflict issue of the law applicable to digital twins. Looking back at the conflict-of-laws evolution in respect of negotiable instruments, it can be observed that the legal recognition of documents of title did not fundamentally disrupt the traditional *lex rei sitae* rule applicable to tangible moveables.[90] In the case of document of titles, it was enough to locate the document instead of the rights they enshrined. The *lex rei sitae* rule simply evolved into a *lex cartae sitae* rule.

Traditionally, the connecting factor to a *res* is indeed territorial (*i.e.* the place where the *res* is located) and not personal. This is because of the singleness of location of a *res* in space-time in contrast with the fact that multiple persons in different jurisdictions may simultaneously have interest or exercise control over the same *res*. Personal connecting factors would be inadequate as it would potentially result in making one single *res* subject to different laws simultaneously, thereby undermining the zero-sum allocation function of property law.

Today, similar situations arise, for instance, in the case of multi-signature agreements that entitle different persons to control the fate of a specific token. Chains of transactions over the same *res* may also lead to situations of conflicting titles. In the case of transfer of tokens recorded on a blockchain, a personal connecting factor (*e.g.* the place of residence of the transferor) would result in a fragmented picture composed of different applicable laws.

Therefore, linking proprietary issues with the law of the place of residence, establishment or main interest of the transferor, the private key holder or more generally of a participant to a DLT system would not be satisfactory.[91] Linking a *res* to one single location in space-time and subjecting it to one single applicable law (the *lex situs*) is paramount to ensure a zero-sum result in line with substantive property law. The *lex situs* rule has also a proven track-record of resilience, resisting even the overhaul forces of the American conflict-of-laws

90 Adrian Briggs, *The Conflict of Laws* (Oxford: OUP 2019), 287 (underlining that the *lex rei sitae* rule applicable in matters of tangible moveables also applies in the case of negotiable instruments where transfer of documents equates transfer of the thing).

91 HCCH (n 27); FMLC (n 33), margin nos. 6.21 – 6.24.

revolution.[92] However, digitalisation and tokenisation now lead to a rethinking of its relevance as the *situs* of securities and now the location of tokens proves difficult to determine. Digitalisation has prompted the search for a novel criterion.

In the case of securities which materialise only in the form of entries in securities accounts or registers, such accounts or registers would provide the necessary anchor to property rights. Where securities are listed in a register held by or on behalf of the issuer, the law of the place of incorporation (*lex incorporationis*) of the issuer would be relevant.

However, to fit the intermediated securities holding system, where securities are held in accounts opened with (a chain of) intermediaries, the Place of the Relevant Intermediary Approach (PRIMA) was retained as the most appropriate connecting factor: the law applicable to proprietary issues shall as a result be the law of the state in which the relevant account is maintained. The rule has been inserted in several European instruments[93] and has been upheld under a "subjective" form (PRIMA+) in the Hague Convention of 5 July 2006 on the Law Applicable to Certain Rights in Respect of Securities held with an Intermediary (Hague Securities Convention).[94]

In the case of tokens taking the form of securities it may be argued that the recording of transactions in DLT systems equate entry into securities accounts or registers for the purpose of securities laws and regulations.[95] At

92 Van Erp (n 31).

93 Article 9(2) of the Settlement Finality Directive (n 78); Article 9 of the Financial Collateral Directive (n 79); Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012, [2014] OJ L257/1 ("CSDR"); and also Article 24 of Directive 2001/24/EC of the European Parliament and of the Council of 4 April 2001 on the reorganisation and winding up of credit institutions, [2001] OJ L125/15 ("Winding-up Directive").

94 The Hague Securities Convention (n 45) entered into force on 1 April 2017 but with very limited success: only three states (the United States, Switzerland, and Mauritius) have ratified it. Article 4 provides primarily that the law applicable to proprietary issues in securities is the law chosen as the law applicable to the account agreement or the law otherwise chosen to govern the issues covered by the convention. Article 5 sets out fall-back rules referring to the law of the place of incorporation or the law of the principal place of business of the relevant intermediary.

95 Responses to the European Commission, "Targeted consultation on the review of Regulation on improving securities settlement in the European Union and on central securities depositories" (*EC*) <https://ec.europa.eu/info/consultations/finance-2020-csdr-review_en> accessed 10 October 2021.

the intra-systemic level, legislators must however expressly provide that the registration of digital assets on DLT systems entail the same proprietary consequences as entry into an account. France has, for example, already leaped the gap, but only for unlisted registered securities and only if DLT registers satisfy some identification and transparency requirements.[96]

However, such an account-centered approach may not be suitable for digital twins. Indeed, digital twins fundamentally aim to create a direct link between the issuer and the token holder. Holding of digital twins therefore resembles more a direct holding system than an indirect holding system. The fundamental interest of the token holder is indeed to avail the service, product or proceeds from the issuer, by the redemption of a token, as the case may be.

The place of the issuer master account would thus appear as a particularly relevant connecting factor that has the advantage of reducing the legal risks at the enforcement stage.[97] The issuer may nevertheless mint a token and proceed to its issuance and sale through a digital account opened with a platform incorporated in another jurisdiction. Additionally, minting a token does not equate a book entry in an account held by or on behalf of the issuer. In the absence of an identifiable register mirroring each and any minting and transfer, the geographical location of the issuer "master account" may be impossible to assert; it might even not be the most accurate connecting factor. At the end of the day, it is the issuer itself, directly or via an agent or appointee, that remains responsible for the payment, delivery of the goods, or provision of service.

4.4 *Connecting the Relevant Intermediary*

DLT networks and blockchains are generally viewed as clear manifestations of the phenomenon of disintermediation, *i.e.* the process consisting of cutting off the middleman in order to source financing directly from market investors.[98]

---

96 Articles L.211-3 and L.211-7 of the French *Code monétaire et financier* (n 35) provide for an equivalence between registration on a DLT and entry into a securities book. In absence of a European regime for listed securities, only French law governed, registered, and unlisted securities can be registered on a DLT. Additionally, DLT systems must satisfy the requirements set out in Article R.211-9-7, such as a clear identification of the types and number of securities and their holder, the existence of a continuity plan and the periodic safeguard of data on an external register. As securities are fully dematerialised under French law and thus exist by their sole entry on a securities book or by their registration on a DLT system, security tokens are arguably plain and simple securities.

97 FMLC (n 33), margin no. 6.20. HCCH (n 27).

98 Thierry Bonneau, *Droit Bancaire* (13th edn, Paris: LGDJ 2019), 30 (characterising the opening of money markets and credit provision to non-bank actors as manifestations of the

Thinking of disintermediation as the total absence of intermediaries would however be misleading. Not all intermediaries disappear in the process, and new intermediaries appear. Credit and payment institutions remain important, even if only for the cash leg of transactions over tokens or other virtual assets. In addition, new actors such as crypto exchanges, wallet service providers, market place platforms, *etc.*, have emerged and play a crucial role in the development of crypto ecosystems.

The main difference lies in the nature of risks and the shift of the persons bearing and managing them. In the case of asset tokenisation, digital twins face a multiplicity of risks. The value of a token may vary with the variation of value of the underlying asset, but if a secondary market for digital twins exists, value variations of the tokens may also be unrelated to the underlying asset.

In such a case, market risks would increase and would also cause issues if digital twins are used as collateral. Token holders also face important counterparty risks, pertaining both to the token layer (*e.g.* default of the market place platform) and the underlying layer (*e.g.* default of the person manufacturing or possessing a tangible good). However, the core risks in matters of asset tokenisation are sustained by the persons or entities whose role is to relay and convey the consequences of transfers of tokens into the real world. Such risks may materialise in particular at the stage of minting/redemption of tokens and when it comes to enforce the title of token holders. It is therefore paramount to clearly identify the persons or intermediaries involved at these stages for both civil law and regulatory purposes.

Regulatory law cannot and should not be blind to the risky nature of such activities. Regulators are likely to impose specific regulatory requirements for both market stability and investor/consumer protection reasons. Issuer of digital twin tokens should however be distinguished from custodians of the underlying asset, wallet service providers, and market place platforms. Custodians of the underlying asset may have possession but are not necessarily the owners of the underlying asset. Most importantly, they may be totally foreign to the process of asset tokenisation. Wallet service providers may provide custody services for digital twins and other virtual assets, but are not directly involved in the tokenisation process. Similarly, platforms may technologically enable the minting, offer and trading of digital twins, but are not responsible for the operative decision to do so. This explains why terms of service of NFTs trading platforms generally disclaim any liability arising from the invalid transfer of

phenomenon of disintermediation). Thierry Bonneau et al. (n 38), 76 (designating financial disintermediation as the process of offering securities without intermediaries).

rights in the underlying asset or from copyright infringements.[99] It is therefore argued that digital twin issuers and related third parties should be subject to regulatory requirements and would be the most relevant anchor of proprietary rights.

Liechtenstein's Blockchain Law is particularly interesting in this respect to the extent that it created a new regulated status of "Physical Validator" as a sub-category of "TT [Trustworthy Technology] Service Provider." The law defines a Physical Validator as "a person who ensures the enforcement of rights in accordance with the agreement, in terms of property law, represented in Tokens on TT [Trustworthy Technology] systems."[100]

Such Physical Validators are thus deemed to play a key function in a tokenised economy, since they are in charge of reconciling token ownership with the effective ownership of the underlying asset which they may keep in custody or have secured through appropriate contractual arrangements.[101] The key role of such intermediaries explains why they are subject to regulatory obligations such as internal control mechanisms[102] and minimum capital requirements.[103] Both natural and legal persons may act as Physical Validator under the law, however it is interesting to note that to date only one entity has been registered under this status in the public register of the Liechtenstein Financial Market Authority (Liechtenstein FMA).[104] This is not so surprising, as asset tokenisation is still at the embryonic stage.

Also, it is important to recall the territorial limitation of regulatory laws and regulations. The status of Physical Validator indeed applies solely to persons having their headquarters or their place of residence in Liechtenstein.[105] Persons performing the role of Physical Validators may well be located abroad – even more so since the location of a Physical Validator does not bear

99 See for instance the terms of service of the Rarible platform (Rarible, "Meet $RARI – Raible Protocol DAO Governance Token" (*Rarible*) <https://rarible.com/rari> accessed 6 June 2022), or of the OpenSea platform (OpeanSea, "Terms of Service" (*OpenSea*, 31 December 2021) <https://opensea.io/tos>).

100 Liechtenstein Blockchain Law (n 35), Article 2(1)(p).

101 Thomas Nägele and Patrick Bont, "Tokenized structures and assets in Liechtenstein law" (2019) 25 Trusts & Trustees 633.

102 Liechtenstein Blockchain Law (n 35), Article 17.

103 *Id.*, Article 16(1)(e) (minimum capital requirements being set at 125,000 Francs if the value of the guaranteed property does not exceed 10 million Francs, and at 250,000 Francs if the value of the guaranteed property exceeds 10 million Francs).

104 Finanzmarktaufsicht Liechtenstein (FMA), „Liechtenstein FMA Register" (*FMA*) <https://fmaregister.fma-li.li/search?searchText=&number=&category=131547> accessed 22 March 2023.

105 Liechtenstein Blockchain Law (n 35), Article 12.

consequences as to whether or not Liechtenstein's token-specific private law regime is triggered.[106] It also follows that, in practice, a Liechtenstein regulated Physical Validator would be expected to determine the relevant private law regime to ensure that the token holder is the rightful owner and has indeed title to the underlying asset.

The Liechtenstein Trustworthy Technologies Act provides nevertheless an interesting connecting factor by coupling the regulatory approach with the conflict-of-laws approach. Article 3(2) of the Liechtenstein Act sets out two alternative connecting factors determining the application of Liechtenstein private law, namely where: 1) the parties to a legal transaction over tokens have expressly elected Liechtenstein specific civil law regime; or 2) a service provider issuing or generating tokens has his/her/its headquarters or place of residence in Liechtenstein.

Such a unilateral conflict-of-laws approach pairs well with the unilateral and territorial regulatory approach. Some difficulties must however be pointed out. First, absent any hierarchy between the two criteria the rule clearly aims to favour the application of Liechtenstein law. This means that even if parties have expressly made another choice than Liechtenstein law to govern their relationship, Liechtenstein law would still be applicable if the issuer or generator of the traded tokens is in Liechtenstein. Such a solution may diametrically run counter the parties' legitimate expectations. There may be good policy reasons to subject private law issues of token transfers to the law of the state where the token issuer has its seat. However, allowing parties to choose Liechtenstein law and not recognising the choice of another state's law when tokens are issued by a natural or legal person on Liechtenstein soil would be at odds with the objectives of legal predictability and international harmony of solutions. Another reason for such constraint on party autonomy may be the lack of an analogous token-specific private regime in foreign substantive laws. This notwithstanding, if similar conflict-of-laws rules are adopted by other legal systems, clashes seem inevitable.

However, the difficulties linked to the approach adopted by Liechtenstein are not insurmountable. Regulatory issues may generally be separated from private law issues. This means that a conflict-of-laws rule does not need to follow a territorial or unilateral approach. The connecting factors adopted by the Liechtenstein legislator could potentially become bilateral.

106 *Id.*, Article 3 (only the circumstance that a regulated service provider issuing or generating tokens with headquarters or place of residence in Liechtenstein shall trigger Liechtenstein special civil law regime).

The question, however, of which connecting factor is the most appropriate would require further consideration. A subjective factor leaving the choice of the applicable law to the token issuer may not be universally accepted, irrespective of whether regulatory law restricts such choice. The lack of success of the Hague Securities Convention that tries to accommodate freedom of choice of law with regulatory considerations (*e.g.* by pointing to the law of the jurisdiction where the relevant intermediary has a qualifying office) provides a clear warning of the risks of any similar approach. However, contrary to the choice of law governing an account agreement, the minting of tokens through smart contracts allows the issuer to insert, from the outset, a choice of law in the metadata file linked to each single token. The choice of law would then be good-against-the-world and certain for any token holder. It should also be observed that it would be in the interest of the issuer to choose a law enabling title over tokens to convey rights in the underlying asset, failing which the issuer would lose its business case and potentially face sanctions for fraud and misrepresentation.

Yet, lacking an express choice of law, or where the choice of law is impracticable, objective factors would be needed. To such end, the domicile, the place of habitual residence, or the place of main interest of the issuer could be relevant connecting factors. If the issuer is a corporation or another type of legal entity, the place of incorporation, the place of central administration, or the main place of business may qualify as relevant connecting factors. It is worth highlighting, however, that a bilateral conflict-of-laws rule built around such objective connecting factors would be workable only upon the assumption that the applicable law contains material provisions having the effect of imposing on the issuer (or any other designated person) an obligation to ensure that title over the tokens effectively conveys rights in the underlying asset. The issuer (or any other related and designated person) would thus be required to make the necessary legal arrangements to ensure that the rights to which the token holder is entitled are enforceable. The issuer may or may not be the direct owner of the underlying asset(s), but should be required by domestic law to ensure (legally and practically) that title to the rights in the underlying asset is irrevocably passed onto the token holder. The validity of said legal arrangements will be determined pursuant to the law of the place of the issuer, including, where applicable, its conflict-of-laws rules. Any failure by the issuer (or other relevant person) to satisfy such obligations would give rise to a claim of the token holder against the issuer under the conditions set forth under domestic law. It is, therefore, argued that the law applicable to proprietary issues of digital twins are better determined by either the conflict-of-laws rules (applicable by *renvoi*) or the substantial provisions (if a specific

regime exists) of the law of the place of residence or establishment of the issuer. This approach would allow, at least, for an allocation of legal authority in line with the nature of property law, as inter-systemic coordination is ensured by one single law: that of the issuer or related relevant person.

The Swiss DLT Act is interesting to the extent that it devised a somewhat conceptually close solution. The DLT Act introduced a new Article 145a into the Swiss Federal Law on Private International Law (LDIP)[107] to subject the conditions of representation and transfer of a right *in personam* to the law designated in the instrument containing or representing such right. The instrument may be a paper certificate or any other equivalent, including DLT tokens. This means that, under Swiss law, it is primarily the law chosen and incorporated in a token (or possibly its accompanying documentation, such as the related white paper) which will determine whether the token effectively represents such right and whether the transfer of the token conveys the transfer of the underlying right. In the absence of a specific choice of law, Article 145a LDIP designates the law of the state of establishment or habitual residence of the issuer as the applicable law. Interestingly, Article 106(1) LDIP, as amended by the Swiss DLT Act, refers to the conflict-of-law rule of Article 145a LDIP to determine whether an instrument (including a DLT token) represents a good. In other words, real rights in a good may be represented in the form of tokens if such representation is allowed by the law chosen and inscribed in the tokens itself (or its accompanying documentation), or by the law of the place of establishment or habitual residence of the issuer if no choice of law has been expressed. Such a conflict-of-law approach is perfectly congruent with the domestic provisions introduced by the Swiss DLT Act which allow goods to be represented in the form of DLT tokens, provided however that all characteristics and debentures are also recorded in the DLT system or its accompanying documentation.[108] However, to settle any priority issue of the rights claimed on a good, Article 106(3) LDIP preserves the application of the *lex rei sitae*. Thus, and in contrast to the approach promoted above, Swiss law does not contemplate the application through *renvoi* of the conflict-of-law rules (including the *lex rei sitae*) of the law of the place of establishment or habitual residence of the issuer. The conflict solution retained under Swiss law is understandably founded on the presumption that foreign legal systems are equivalent to

107 Swiss Federal Law on Private International Law (LDIP) of 18 December 1987, AS 1988 1776, SR 291.

108 Article 1153a Swiss Code of Obligations (Federal Act on the Amendment of the Swiss Civil Code (Part Five: The Code of Obligations) of 30 March 1911 (Status as of 1 January 2022), AS 27 317, SR 220.

Swiss law,[109] but it remains that legal systems may, in practice, devise different solutions or may choose only to address certain aspects of asset tokenisation, thereby leaving room for conflict-of-laws rules to apply. It is, therefore, submitted that conflict-of-law rules of the law of the place of habitual residence or establishment of the issuer should also be applied by *renvoi*, when and where relevant.

Concerns over the identification of the issuer may also arise, but they must not be exaggerated. While DLTs allow for persons to transact under pseudonyms or anonymously, it is not necessarily so. If businesses intend to resort to asset tokenisation to do business, it is unlikely that they will remain anonymous. Even in the case of natural persons, if they intend to mint a token, they will connect their wallet (*e.g.* Metamask) supporting a cryptocurrency such as Ethers to a digital platform where a token can be minted and offered for sale.[110] Identification of the issuer would then be facilitated by the fact that gatekeepers such as crypto exchanges and wallet service providers are increasingly under the yoke of anti-money laundering and combating the financing of terrorism (AML-CFT) requirements, including *inter alia* know-your-customer (KYC) due diligence and suspect activity reporting obligations.[111]

Yet, in case of absolute impossibility to identify the issuer of a digital twin, fall-back rules should be devised. At first sight, the most relevant intermediary is then the DLT-based platform which enables the minting and trading of tokens. DLT platforms in this context should be distinguished from the DLT systems mentioned above. Several DLT platforms may indeed develop on the basis of the same DLT system or blockchain infrastructure (*e.g.* Ethereum blockchain). The possible connecting factors outlined above (*i.e.* elective *situs*, modified elective *situs*, PROPA, PREMA, in particular) would then apply *mutatis mutandis*. However, the same criticism would also apply. Even if the terms and conditions of DLT platforms expressly stipulate a choice of law, proprietary issues are generally excluded; and this for a good reason in the context

109 Among others, Marie-Laure Niboyet and Géraud de Geouffre de la Pradelle, *Droit International Privé* (6th edn, Issy-les Moulineaux: LGDJ 2017), 141, no. 175 (outlining the need for any bilateral conflict-of-law system to postulate that legal systems are, in principle, equivalent).

110 See, among others: OpenSea (n 89).

111 See Article 2(g) and (h) Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, amended by Directive (EU) 2018/843 of 30 May 2018 and by Directive (EU) 2019/2177 of 18 December 2019, [2015] OJ L141/73 (AMLD consolidated).

of digital twins, since DLT platforms do not normally have any power over the underlying asset. The same remark applies if the law of the place of incorporation of the DLT platform is deemed applicable. In such cases, the only viable solution (especially if the underlying asset is a tangible moveable or immoveable) would seem to be to apply the *lex rei sitae* of the underlying asset.

5 Conclusion

Taking stock of the fast development and economic relevance of asset tokenisation, this contribution has sought to analyse and provide tentative approaches to proprietary and conflict-of-laws issues relating to tokenised assets or digital twins. It is argued that if asset tokenisation is to bring any economic benefit at all, legal systems should introduce legal provisions to the effect of recognising the validity and effect of the transfer of tokens (or digital twins) over the rights in an underlying off-chain asset.

The nature of tokens (or digital twins) as financial intangible *res* should also be acknowledged. Although harmonisation projects are underway, the risks of legal fragmentation are serious. Conflict of laws may, however, play an important part in reducing such risks and providing more legal certainty and predictability of outcomes. To that end, doubts have been raised as to whether the simple application of the *lex rei sitae* of the underlying asset of digital twins would lead to favourable results.

Other possible connecting factors proposed to connect virtual assets, including digital twins, have been reviewed, without leading, however, to a conclusive result. It has been proposed, instead, to connect digital twins, primarily, either to the law chosen by the issuer and incorporated in the metadata of the token itself, or, in the absence of choice of law or in case of impracticability, to the law (including its conflict rules, where applicable) of the place of habitual residence of the issuer (place of incorporation, place of central administration or main place of business for legal entities).

The identity and location of the issuer may sometimes be difficult to determine, but should not be an impossible task in most cases. If identification of the issuer is nonetheless impossible to establish with certainty, the last resort and most appropriate connecting factor would remain the *lex rei sitae* of the underlying, especially if the asset tethered to a token is a tangible moveable or immoveable.

Although some possible approaches may be sketched out and assessed, it is ultimately for legislators to take a position and introduce new rules tailored to the needs of an increasingly tokenised economy.

CHAPTER 11

Cryptocurrencies and Conflict of Laws

Francesca C. Villata

1 Introductory Remarks on Cryptocurrencies and PIL Issues

According to Coinmarketcap,[1] as of November 2021 over 7700 different cryptocurrencies are traded globally and the worldwide crypto market cap amounts to USD 2.47 trillion. Among them, Bitcoin is the best known[2] and most present on the market, with a market share of around 45% (even 65% in June 2020).[3] Moreover, Bitcoin was not only the prototype of all cryptocurrencies, revealed to the world by the legendary[4] Satoshi Nakamoto on 31 October

1 CoinMarketCap, "Today's Cryptocurrency Prices by Market Cap" (*CoinMarketCap*) <https://coinmarketcap.com/> accessed 27 November 2021.

2 *Wright v McCormack* [2021] EWHC 2671 (QB) para. 5, whereby "[a] cryptocurrency is a digital asset designed to work as a medium of exchange, in which individual coin ownership records are stored in a ledger existing in a computerised database using cryptography to secure transactions, to control the creation of additional coins, and to verify the transfer of coin ownership. It does not exist in physical form (as paper money does) and is typically not issued by a central authority. Bitcoin is probably the best-known cryptocurrency." See also Michael Karim and Gergana Tomova, "Research Note: Cryptoasset consumer research 2021" (*Financial Conduct Authority*, 17 June 2021) <https://www.fca.org.uk/publications/research/research-note-cryptoasset-consumer-research-2021>.

3 European Parliament resolution of 8 October 2020 with recommendations to the Commission on Digital Finance: emerging risks in crypto-assets - regulatory and supervisory challenges in the area of financial services, institutions and markets (2020/2034(INL)), P9_TA(2020)0265, Recital N.

4 "Satoshi Nakamoto" is the pseudonym used by the person, or persons, who developed Bitcoin. In that regard, a dispute was filed before English courts between Dr. Craig Wright, a national of Australia who has lived in the United Kingdom since December 2015 and is a computer scientist with a particular interest in cryptocurrencies, including Bitcoin, maintaining that he is Satoshi Nakamoto, and Roger Ver, a bitcoin investor and commentator on bitcoin and other cryptocurrencies, who was born in California, U.S., and moved to Japan, which he described in evidence as the global centre for cryptocurrencies, in 2005. In 2014 he renounced his US citizenship and became a citizen of St. Kitts & Nevis, although he continues to live in Japan. Mr. Ver does not accept that Dr. Wright is Satoshi Nakamoto. Dr. Wright claims that he was libeled by Mr. Ver in a YouTube video posted on the Bitcoin.com YouTube channel, a tweet containing the YouTube video, and a reply on Mr. Ver's Twitter Account posted from Bkk-Shadow some 8 minutes after the tweet from Mr. Ver. These publications were alleged to be defamatory, in that Dr. Wright "had fraudulently claimed to be Satoshi Nakamoto, that is to say the person, or one of the group of people who developed Bitcoin." *Cf. Wright v Ver* [2020]

© FRANCESCA C. VILLATA, 2023 | DOI:10.1163/9789004514850_013
This is an open access chapter distributed under the terms of the CC BY-NC-ND 4.0 license.

2008,[5] but it also represents the paradigm around which the legal discourse on distributed ledger technologies (DLTs) and crypto assets was, at least initially, developed.

Technological features of cryptocurrencies have been raising a number of challenges for lawyers and, namely, for experts in Private International Law (PIL),[6] in that (i), cryptocurrencies are intangible, (ii) they exhibit a wide range of different financial features[7] that, to add further complexity, evolve in parallel with technological developments, (iii) the identity of cryptocurrency users – *i.e.*, everyone who is involved in the process of creation and transfer of cryptocurrencies[8] – is, at minimum, not easy to trace, since identities are protected through pseudonyms[9] or, even, full anonymity, (iv) they are set for more than one usage, *i.e.*, both as a payment instrument and a form of investment (albeit a very risky one!).[10] Even more relevant, (v) they intrinsically have a

---

EWCA Civ 672 (29 May 2020) declining English jurisdiction on the controversy, based on the argument "that England and Wales is not clearly the most appropriate place to bring this action for defamation." Furthermore, Dr. Wright also sued journalist Peter McCormack for defamation in 2019 over tweets or, a series of tweets, he had made in which he either directly, or by innuendo, called Wright a fraud for his claim that he was Bitcoin inventor Satoshi Nakamoto: *cf. Wright v McCormack* [2021] EWHC 2671 (QB).

5 Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (*Bitcoin*, 24 May 2009) <https://bitcoin.org/bitcoin.pdf>.

6 The present paper has benefitted from the research conducted within the framework of the Project Time to Become Digital in Law – DIGinLaw - KA226 (Call 2020 Round 1 KA2 - Cooperation for innovation and the exchange of good practices).

7 *Cf.* European Central Bank (ECB), "Virtual currency schemes – a further analysis" (*ECB*, February 2015), 9 ff <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf> accessed 30 November 2021; and Robby Houben and Alexander Snyers, "Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion" (*European Parliament*, July 2018), 31 ff <https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf> accessed 30 November 2021, providing a synthetic description of the 10 cryptocurrencies with the highest market capitalisation.

8 Yet, Article 4 of the Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets (recast), [2021]

9 COM/2021/422 final, 2021/0241(COD) requires that the crypto asset service provider of the originator ensures that transfers of crypto assets are accompanied by the name of the originator, the originator's account number, where such an account exists and is used to process the transaction, and the originator's address, official personal document number, customer identification number or date and place of birth. Moreover, the crypto asset service provider of the originator must ensure that transfers of crypto assets are accompanied by the name of the beneficiary and the beneficiary's account number, where such an account exists and is used to process the transaction.
See Kleczewski in this book, 128 ff.

10 European Parliament resolution of 8 October 2020 (n 3), Recital L.

cross-border reach, since they are based on decentralised distributed ledgers, potentially spanned all over the world, with no connections to any particular state, allowing value to be transferred between users across borders at a very high speed, not conditional on the location of the transferor and the transferee. Finally, (vi) it is extremely difficult to impose legal restrictions on their circulation, including territorial restrictions, not only because of the decentralised nature of said ledgers, but also because of their inherent autonomy *vis-à-vis* the law. In fact, certain technical features of the systems on which the mere existence of cryptocurrencies depend, such as the automated functioning of those systems – based on smart contracts, as well as on consent mechanisms relying on cryptographic techniques, collective validation of the transactions, and continuous chains of blocks, unmodifiable without the consent of the majority of participants to the system (or good hacking skills…) –, make those systems not only tamper resistant, but also difficult to subject to any legal constraints.

Looking at cryptocurrencies from a legal perspective, according to the many definitions provided by various institutional players, in their attempt to grasp the distinctive features of cryptocurrencies that are relevant for the purpose of establishing a sound and effective legal framework, coherent with the policy objectives pursued by those institutions, the following elements have been commonly identified.

Firstly, the core of all definitions, including legislative ones,[11] lies in the notion of cryptocurrencies as digital representations of

11 Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, [2015] OJ L41/73, as amended by Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018, [2018] OJ L156/43, and Directive (EU) 2019/2177 of the European Parliament and of the Council of 18 December 2019, [2019] OJ L334/155, art. 3 n 18 ("'virtual currencies'" means a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically") and Recital 10; *cf, e.g.*, the Italian implementing rule provided in *decreto legislativo* n 231 of 21 November 2007, *Gazz. Uff.* N 290 of 14 December 2007 Suppl. Ord. n 268, art. 1 para. 2 *litt.* Qq, as amended by art. 1 para. 1 *litt* h of *decreto legislativo* n 125 of 4 October 2019, *Gazz. Uff.* n 252 of 26 October 2019: "valuta virtuale: la rappresentazione digitale di valore, non emessa né garantita da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di

value,[12] originated in distributed ledgers via a process called "mining,"[13] making use of those ledgers to allow remote peer-to-peer exchanges of that value[14] and relying on cryptographic techniques to achieve consensus on the validation of the transfer.[15] Cryptocurrencies are not *per se* legal tender (unless any state or other monetary authority establish that they are),[16] neither are they issued by a central bank or public authority,[17] nor necessarily attached to a fiat

---

scambio per l'acquisto di beni e servizi o per finalità di investimento e trasferita, archiviata e negoziata elettronicamente." See also Uniform Law Commission, Uniform Regulation of Virtual-Currency Businesses Act (URVCBA), Sec. 102 n 23: "'Virtual currency:' (A) means a digital representation of value that: (i) is used as a medium of exchange, unit of account, or store of value; and (ii) is not legal tender, whether or not denominated in legal tender;" Matthias Lehmann, "National Blockchain Laws as a Threat to Capital Markets Integration" (2021) Uniform Law Review 148, 162 ff.

12 Dong He et al., "Virtual Currencies and Beyond: Initial Considerations (IMF Staff Discussion Note)" (*International Monetary Fund*, January 2016), 7 <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf> accessed 27 November 2021; European Banking Authority (EBA), "EBA Opinion on 'Virtual Currencies'" (*EBA*, 4 July 2014), 11, para. 20 <https://www.eba.europa.eu/sites/default/documents/files/documents/10180/657547/81409b94-4222-45d7-ba3b-7deb5863ab57/EBA-Op-2014-08%20Opinion%20on%20Virtual%20Currencies.pdf?retry=1> ("EBA Opinion"): "This part of the definition refers to the fact that the value is essentially represented in digital form. This does not exclude the possibility that it may also be physically represented, such as through paper printouts or an engraved metal object. The term 'digital representation of value' is close to the monetary concept of a 'unit of account' but includes the option to consider VCs as private money or a commodity. It also avoids making reference to a standard numerical unit of account for the measurement of value and costs of goods, services, assets and liabilities, which might (according to some views), imply that it needs to be stable over time."

13 Houben and Snyers (n 7), 32.

14 Bank for International Settlements, Committee on Payments and Market Infrastructures, "Digital Currencies" (November 2015), 5 <https://www.bis.org/cpmi/publ/d137.htm>; Caroline Kleiner, "Cryptocurrencies as Transnational Currencies?," in Christoph Benicke and Stefan Huber (eds), *National, International, Transnational: Harmonischer Dreiklang im Recht. Festschrift für Herbert Kronke zum 70. Geburtstag* (Ernst and Werner Gieseking 2020), 979 ff.

15 World Bank Group (Harish Natarajan, Solvej Krause, and Harish Gradstein), "Distributed Ledger Technology (DLT) and blockchain (FinTech Note No. 1)" Washington, (*World Bank*, 2017), IV <http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf> accessed 27 November 2021.

16 On 7 September 2021, El Salvador became the first country to adopt Bitcoin as a legal tender. See *infra* (n 50).

17 European Securities and Markets Authority (ESMA), European Banking Authority (EBA), and European Insurance and Occupational Pensions Authority (EIOPA), "ESMA, EBA and EIOPA warn consumers on the risks of Virtual Currencies" (*ESMA*, 12 February 2018), 1

currency,[18] but they may well be converted into fiat currencies and vice versa,[19] their economic value being determined by supply and demand.[20] Accordingly, despite their volatility,[21] cryptocurrencies are "designed to work as a medium of exchange"[22] and, actually, as acknowledged by certain pieces of legislation, are "accepted by natural or legal persons as a means of exchange and… can be transferred, stored and traded electronically."[23] Moreover, in fact, cryptocurrencies may represent an investment vehicle, though a rather risky one, whereby their status as a store of value is largely dependent on their success as medium of exchange, hence, the rise of stablecoins, which are established with the purpose of eliminating the volatility of traditional cryptocurrencies by consistently holding a stable value. In most cases, one unit of a stablecoin is "pegged" at the value of the US dollar or the Japanese yen (fiat-backed).

The aforementioned characteristics of cryptocurrencies and, in particular, their intrinsic cross-border reach prompt the question of their PIL regime and, namely, (i) the need to identify, among the existing PIL rules, those which are applicable to transactions involving cryptocurrencies, both as payment instruments and as (possible) store of value, and to investigate whether those rules are suitable for framing them, either in terms of legal characterisation or of connecting factors and other techniques to establish the applicable law. If, and to the extent that the answer to the first question is negative, this paper

<https://www.esma.europa.eu/sites/default/files/library/esma50-164-1284_joint_esas_warning_on_virtual_currenciesl.pdf>.

18 EBA Opinion (n 12), 7. According to the European Central Bank (European Central Bank, "Virtual Currency Schemes" (*ECB*, October 2012), 14 https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf accessed 27 November 2021), cryptocurrencies fall under the notion of "virtual currency schemes with bidirectional flow," in that users can buy and sell virtual money according to the exchange rates with their currency so that the virtual currency is "similar to any other convertible currency with regard to the interoperability with the real world;" *cf.* Houben and Snyers (n 7), 21–22; Roberto Bocchini, "Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche" (2017) 27 Il diritto dell'informazione e dell'informatica 39.

19 Houben and Snyers (n 7), 23.

20 Bank for International Settlements (n **14**) 4; Financial Markets Law Committee, "Issues of Legal Uncertainty Arising in the Context of Virtual Currencies" (*FMLC*, July 2016), 4 <http://fmlc.org/wp-content/uploads/2018/03/virtual_currencies_paper_-_edited_january_2017.pdf> accessed 27 November 2021.

21 See, *e.g.*, European Central Bank (n 7), 16.

22 *Wright* (n 2).

23 Directive (EU) 2015/849 (n 23), art. 3 n 18; European Parliament resolution of 26 May 2016 on virtual currencies, [2016] OJ/C 76 (2018/C 076/13); *decreto legislativo* n 90 del 25 maggio 2017 , art. 1 para. 2 *litt* qq, Gazzetta Ufficiale n 140, 19 June 2017 - Suppl. Ord. n 28.

will then explore (ii) if cryptocurrencies deserve, also in light of their growing economic relevance, or require, because of their potential systemic relevance, differentiated PIL rules, not only in comparison to traditional assets, but also in relation to other crypto assets, depending upon their intrinsic technical features and/or their use case, and (iii) whether territorial connecting factors are still relevant for or can apply at all to that context or, instead, whether different (combinations) of PIL techniques could be more fit for purpose.

The first obstacle on the road to determining the law applicable to cryptocurrencies, and, more generally, to the DLT ecosystem, has often been identified in its autonomy: notably, such opinion is premised on the fact that technology operates independently from the law, according to internal cryptographic protocols and mechanisms of consent-validation, in principle without considering whether the outcomes of those processes are legally sound. Moreover, distributed ledgers are often seen as "immutable," although the data contained in such networks can indeed be manipulated in extraordinary circumstances, such as a collusion between participants to the network. Actually, the tamper-evident nature of DLTs and, particularly, blockchains, – linked with the cryptographic hash-chaining following the creation of a new block[24] – means that there are often "no technical means, short of undermining the integrity of the entire system, to unwind a transfer."[25] Because blocks are linked through hashes, changing pieces of information that constitute the hashes is difficult and expensive, although not impossible.[26] This creates regulatory challenges, for example, to enforce a court order. Moreover, where a smart contract is embedded in the blockchain to perform part of a transaction, its functioning cannot in principle be halted, or reversed, even where prescribed by law (at least in a public permissionless chain, whilst in a private permissioned chain such modifications are said to be more feasible). Although it is possible to incorporate exceptions or conditions into a smart contract to align with legal provisions, such flexibility should, in any case, be coded into the smart contract at the outset, which takes away from the decentralisation and efficiency that make smart contracts attractive.[27]

---

24 Michèle Finck, *Blockchain Regulation and Governance in Europe* (Cambridge University Press 2018), 5.

25 Kevin Werbach and Nicolas Cornell, "Contracts Ex Machina" (2017) 67 Duke Law Journal 313, 335.

26 Amanda Anderberg et al., *Blockchain Now And Tomorrow: Assessing Multidimensional Impacts of Distributed Ledger Technologies*, Susana Nascimento and Alexandre Pólvora (eds) (Publications Office of the European Union 2019), 16 ff.

27 Werbach and Cornell (n 25), 335.

Notwithstanding the aforementioned technical difficulties and irrespective of both the expectations of the participants to a blockchain system and certain scholarly assertions,[28] blockchain transactions cannot, actually, eschew the law, nor should parties to those transactions have an interest in keeping completely away from the law: at least, this is the case insofar as they wish to be able to rely on the enforcement mechanisms that only state authority has the power to operate, should any player involved in said transactions behave unfairly or be unable to perform its functions in the relevant transaction scheme.[29] Therefore, the present paper aims to provide some (tentative) answers to the three questions set out above, starting from the basic issue of characterisation.

2 Characterisation of Cryptocurrencies

From a legal perspective, the classification of cryptocurrencies is (very) far from being definite, let alone uniform, under domestic laws.

2.1 *"Cryptocurrencies" under National Substantive Laws*

English case-law and scholars have progressively converged on the idea of a cryptocurrency as a "particularly odd type of incorporeal"[30] or "intangible personal property," insofar as, unlike *choses* in action, they do not themselves constitute a right which has a concomitant obligation in another.[31] Namely, cryptocurrencies are deemed to possess the characteristics of property, as summarised in *National Bank v Ainsworth*,[32] which entails that they are "definable, identifiable by third parties, capable in [their] nature of assumption by third parties and have some degree of permanence and stability" according to the assessment conducted by the UK Jurisdiction Taskforce[33] endorsed by

28 Aaron Wright and Primavera De Filippi, "Decentralized Blockchain Technology and the Rise of Lex Cryptographia" (*SSRN*, 10 March 2015), 48 <https://papers.ssrn.com/abstract=2580664>.

29 See EBA Opinion (n 12), 23 ff for an assessment of risks that can arise from virtual currencies.

30 Daniel Carr, "Cryptocurrencies as Property in Civilian and Mixed Legal Systems," in David Fox and Sarah Green (eds), *Cryptocurrencies in Public and Private Law* (OUP 2019), 180 f para. 7.07.

31 David Fox, "Cryptocurrencies in the Common Law of Property" in David Fox and Sarah Green (eds), *Cryptocurrencies in Public and Private Law* (OUP 2019), 150 ff.

32 *National Provincial Bank v Ainsworth* [1965] UKHL 1, 19.

33 Financial Markets Law Committee (n 20), 5, 23; UK Jurisdiction Taskforce, "Legal statement on crypto-assets and smart contracts" (*Tech Nation*, November 2019), 49–57

subsequent jurisprudence.[34] Following a call for evidence, on 24 November 2021 the Law Commission published an "Interim Update" concerning the

<https://technation.io/about-us/lawtech-panel> accessed 5 June 2022. The UK Jurisdiction Taskforce is one of the six taskforces of the LawTech Delivery Panel within The Law Society of England and Wales. According to the website of The Law Society (<https://www.lawsociety.org.uk/campaigns/lawtech/guides/lawtech-delivery-panel>), the LawTech Delivery Panel is "a team of industry experts and leading figures from government and the judiciary, has been formed to help the UK legal sector grow and fulfil its potential. By identifying both barriers to and catalysts for growth, the panel will provide direction to the legal sector and help foster an environment in which new technology can thrive." The position taken by the UK Jurisdiction Taskforce had been anticipated, albeit concisely, in a couple of judgments: *Vorotyntseva v MONEY-4 Ltd* (*t/a nebeus.com*) *& Ors* [2018] EWHC 2596 (Ch), 13; *Liam David Robertson v Persons Unknown* (unreported), quoted *in AA v Persons Unknown & Ors, Re Bitcoin* [2019] EWHC 3556 (Comm), 13.

34 *Ion Science & Duncan Johns v Persons Unknown* (unreported) (21 December 2020), 13, as summarised by Lorna Sleave, "Cryptocurrency Fraud - The High Court Considers The Position Of 'Crypto-assets'" (Mondaq Business Briefing, 6 May 2021) <https://link.gale.com/apps/doc/A663644295/ITOF?u=milano&sid=bookmark-ITOF&xid=03ffe69d>. The case is said to have arisen from proceedings brought by Ion Science Limited (ISL) and its sole director Duncan Johns, who claimed to be victims of a cryptocurrency initial coin offering, or ICO, fraud. Mr. Johns claimed he was persuaded by an individual, Ms. Black, said to be connected to a Swiss entity called Neo Capital, to transfer funds which were converted into Bitcoin by Ms. Black, granting Ms. Black remote access to his computer to manage this. Mr. Johns also made further transfers to an escrow account, claiming Ms. Black informed him these payments were needed to release commission payments from one of the investments, the Oileum ICO. Allegedly, the applicants subsequently discovered that Neo Capital was not a real company and that the Swiss regulator had issued a warning that it may be providing unauthorised services. Neither Mr. Johns nor ISL received any profits supposedly made in relation to the Oileum ICO or received back any of the funds invested. The court heard evidence from an expert in cryptocurrency fraud who concluded that (i) a substantial part of the bitcoins transferred or their traceable proceeds were held by the Binance and Kraken cryptocurrency exchanges; and (ii) both exchanges held information about the customers to whom those accounts belong. Alleging the sums invested had been misappropriated, the applicants applied for a proprietary injunction, a worldwide freezing order, and an ancillary disclosure order against persons unknown, the individuals or companies describing themselves as being or connected to Neo Capital. In addition, the applicants sought a disclosure order against Binance Holdings Limited, a Cayman company believed to be the parent of the group of companies that operates the Binance Cryptocurrency Exchange and Payments Ventures, a US entity believed to be the parent of the group of companies that operates the Kraken Cryptocurrency Exchange. The applicants further asked for permission to serve the proceedings out of the jurisdiction and by alternative means. Drawing (also) on analysis of the position in the UK Jurisdiction Taskforce (n 33), the court found there was at least a serious issue to be tried that Bitcoin was property under the common law definition. See also *AA* (n 33), 59; *Fetch.AI Lrd & Anor v Persons Unknown Category A & Ors* [2021] EWHC 2254 (Comm), 9.

"Digital Asset Project," whereby, while "acknowledging that 'digital asset is an extremely broad term that requires further subdivision,'" it "recognise[d] that certain digital assets could fall within a new 'third category' of personal property." As "indicia" to determine whether or not a digital thing falls within that category the Law Commission proposes the following: (i) that the digital thing has an existence independent of both persons and the legal system, (ii) that the digital thing is rivalrous, *i.e.* that the use or consumption of the thing by one person, or a specific group of persons, inhibits use or consumption of that thing by others, and finally (iii) that the digital thing is fully divestible on transfer.[35] The classification as property has also been upheld by Singapore[36] and Russia,[37] as well as certain Italian judgments.[38]

On the other hand, in the statement above, the UK Jurisdiction Taskforce has included crypto assets in general among "conventional financial assets."[39] Along the same lines, the German Federal Financial Supervisory Authority ("BaFin") issued a communication, according to which "[i]n accordance with BaFin's legally binding decision on units of account within the meaning of section 1(11) sentence 1 of the KWG [Banking Act – *Kreditwesengesetz*], bitcoins are financial instruments" and, namely, "units of account… comparable to foreign exchange with the difference that they do not refer to a legal tender."[40] Following a successful challenge in court, the German legislator has introduced a new provision into the KWG defining crypto assets (*Kryptowerte*) as financial instruments.[41]

---

35 Law Commission, "Digital Assets Interim Update" (*Law Commission*, 24 November 2021), 1.14–1.17 <https://www.lawcom.gov.uk/project/digital-assets/>.

36 *B2C2 Ltd v Quoine Pte Ltd* [2019] SGHC(I) 03, 142, quoting *National Provincial Bank* (n 32).

37 Matthias Haentjens, Tycho De Graaf, and Ilya Kokorin, "The Failed Hopes of Disintermediation: Crypto-Custodian Insolvency, Legal Risks and How to Avoid Them" (2020) Singapore Journal of Legal Studies 526, 551.

38 Trib Firenze 19 December-2018, Contratti 2019, 6, 661 note Domenico Fauceglia, "Il deposito e la restituzione delle criptovalute;" Trib Firenze (Sez fall) 21 January 2019, Giur. It. 2020, 2657, note Domenico Fauceglia.

39 UK Jurisdiction Taskforce (n 33), 52.

40 German Federal Financial Supervisory Authority ("BaFin"), "Virtual Currency (VC)" (*BaFin*, 11 December 2017) <https://www.bafin.de/EN/Aufsicht/FinTech/VirtualCurrency/virtual_currency_node_en.html>. Along the same line of reasoning see Cass pen (2) 17 September 2020 n 26807, Giur It 2021, 2224, note Rosa Maria Vadalà, "La dimensione finanziaria delle valute virtuali. Profili assiologici di tutela penale."

41 See section 1(11) no. 10 of the KWG. In section 1(11) sentence 4 of the KWG, crypto assets are defined as a digital representation of value which has neither been issued nor guaranteed by a central bank or public body; it does not have the legal status of currency or money but, on the basis of an agreement or actual practice, is accepted by natural

Turning to the other side of the Atlantic Ocean, in July 2018 the Uniform Law Commission adopted the "Uniform Supplemental Commercial Law for the Uniform Regulation of Virtual-Currency Businesses Act" ("USCL for URVCBA") and recommended its enactment in all the United States.[42] According to Section 4, by virtue of agreement between parties to virtual currency transactions, the virtual currency may be "treated as a financial asset credited or held for credit to the securities account of the user," thereby collocating said transactions into the realm of Article 8 of the Uniform Commercial Code (UCC). As it has been rightly pointed out, however, the notion of securities entitlement embodied in Article 8 UCC – whereby holders of securities are granted with a claim for securities against the relevant intermediary – seems "incongruous" with the pattern of traceability that is commonly reconnected with crypto assets because of the DLTs supporting the creation and "transfer" of said assets. Therefore, Section 502(a) URVCBA requires that "A licensee or registrant that has control of virtual currency for one or more persons (…) maintain in its control an amount of each type of virtual currency sufficient to satisfy the aggregate entitlements of the persons to the type of virtual currency."[43] Anyway, according to Section 7

---

or legal persons as a means of exchange or payment or serves investment purposes; it can be transferred, stored, and traded by electronic means. See BaFin, "Guidance notice – guidelines concerning the statutory definition of crypto custody business (section 1 (1a) sentence 2 no. 6 of the German Banking Act (Kreditwesengesetz – KWG)" (*BaFin*, 2 March 2020), <https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Merkblatt/mb_200302_kryptoverwahrgeschaeft_en.html?nn=9451720#O4>.

42 The Final Text can be retrieved at the Uniform Law Commission website, namely <https://www.uniformlaws.org/viewdocument/final-act-154?CommunityKey=e104aaa8-c10f-45a7-a34a-0423c2106778&tab=librarydocuments> accessed 20 February 2022. See Zachary Hubbell, "The Uniform Regulation of Virtual-Currency Business Act: Advancing State Regulatory Interests in a Truly Cashless Economy" (2019) 59 Jurimetrics 313.

43 However, whilst Rhode Island enacted the above mentioned provisions of the USCL for URVCBA – namely under R.I. Gen. Laws § 6-56-1-6-56-11 (Current through Chapter 429 (all legislation) of the 2021 Session, including all corrections and changes made by the Director of Law Revision) <https://advance-lexis-com.pros2.lib.unimi.it/api/document?collection=statutes-legislation&id=urn:contentItem:62DF-62M1-DYB7-W0YY-00000-00&context=1516831> accessed 22 February 2022. Wyoming has followed a different approach, whereby a digital asset, even if treated as a financial asset for the purpose of art 8 UCC, shall remain intangible personal property. Moreover, according to said provision, "[v]irtual currency is intangible personal property and shall be considered money;" see § 34-29-102. Classification of digital assets as property; applicability to Uniform Commercial Code; application of other law., Wyo. Stat. § 34-29-102 (Current through 2021 General Session and Special Session of the Wyoming Legislature. Subject to revisions by LSO) <https://advance-lexis-com.pros2.lib.unimi.it/api/document?collection=statutes-legislation&id=urn:contentItem:62DC-SNC3-CH1B-T54F-00000-00&context=1516831> accessed 22

USCL for URVCBA "Treatment of virtual currency as a financial asset credited to a securities account under this [act] and Article 8 does not determine the characterisation or treatment of the virtual currency under any other statute or rule."

In fact, on 10 June 2021, the Securities and Exchange Commission (SEC)'s Office of Investor Education and Advocacy (OIEA) and the Commodity Futures Trading Commission (CFTC)'s Office of Customer Education and Outreach (OCEO) published an "Investor Bulletin," whereby, while urging "investors considering a fund with exposure to the Bitcoin futures market to weigh carefully the potential risks and benefits of the investment," in light of "the volatility of Bitcoin and the Bitcoin futures market, as well as the lack of regulation and potential for fraud or manipulation in the underlying Bitcoin market," expressed the view that "in the United States, Bitcoin is a commodity, and commodity futures trading is required to take place on futures exchanges regulated and supervised by the CFTC."[44] Although the "Investor Bulletin" only represents the views of the staff of the SEC's Office of Investor Education and Advocacy and CFTC's Office of Customer Education and Outreach and it is not a rule, regulation, or statement of the SEC or the CFTC, on 28 September 2021 the latter authority issued an order, filing and settling of charges against Payward Ventures, Inc. d/b/a Kraken, one of the cryptocurrency industry's largest market participants, for offering margined retail commodity transactions in cryptocurrency -– including Bitcoin – and failing to register as a futures commission merchant (FCM).[45]

February 2022. See Lehmann (n 11), 164 f.; Matt Crockett, "Wyoming's DIY Project Gets Western with the UCC" (2020) 20 Wyoming Law Review 105; Sarah Jane Hughes, "Property, Agency, and the Blockchain: New Technology and Longstanding Legal Paradigms" (2019) 65 Wayne Law Review 57. Wyo. Stat. § 34-29-102.

44 The joint statement is contained in US Securities and Exchange Commission, "Funds Trading in Bitcoin Futures – Investor Bulletin" (*SEC*, 10 June 2021) <https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-bulletins/funds>.

45 The CFTC alleged that each of the defendants was acting as an unregistered FCM. Under Section 1a(28)(a) of the Commodity Exchange Act, 7 U.S.C. § 1(a)(28)(A), an FCM is any "individual, association, partnership, or trust that is engaged in soliciting or accepting orders for the purchase or sale of a commodity for future delivery; a security futures product; a swap… any commodity option authorized under section 6c of this title; or any leverage transaction authorized under section 23 of this title." To be considered an FCM, that entity must also "accept money, securities, or property (or extends credit in lieu thereof) to margin, guarantee, or secure any trades or contracts that result or may result therefrom." See 7 U.S.C. § 1(a)(28)(A)(II). 7 U.S.C. § 6d(1) requires FCMs to be registered with the CFTC. See Joseph B. Evans and Alexandra C. Scheibe, "A Flurry of CFTC Actions Shock

A different approach has been followed under the Swiss Act to Adapt Federal Law to Developments in Distributed Ledger Technology ("DLT Act"), some parts of which entered into force on 1 February 2021.[46] That piece of legislation, actually, acknowledges the distinction between tokens in the form of cryptocurrencies, that are classified as intangible assets under civil law, for which that law does not provide any specific requirements nor obstacles to their transfer, and a new category of ledger-based securities (*Registerwertrecht*) that is introduced in the Code of Obligations (*Obligationenrecht*, OR, Art. 622 para 1; Art. 973d).[47] The wording of the provision is technology-neutral and does not mention the term DLT, but describes its characteristics instead. A ledger-based security is defined as a right that, according to an agreement of the parties, is registered in a ledger-based security register and can be asserted and transferred only via this register (Art. 973d para 1 OR). The ledger-based security register must fulfil the following requirements: it gives creditors, but not the debtor, power of disposal over their assets by means of a technical process. Its integrity is protected through appropriate technical and organisational measures to prevent unauthorised modifications, such as joint management by several participants that are independent of each other. The content of the rights, the functioning of the register, and the register agreement are recorded in the register or in the accompanying data. Creditors may access information and register entries that concern them, and may test the integrity of the register entry that concerns them without the help of third parties (Art 973d para 2 OR). Debtors of ledger-based securities are obligated and allowed to render performance only to a creditor whose name is registered in the ledger-based security register (Art. 973e para 1 OR). A *bona fide* purchaser may rely on the content of the register (protection of good faith) (Art 973e para 3 OR). The transfer of the ledger-based security is subject to the terms of the registry agreement (Art. 973f para 1 OR). According to Article 973c ff OR, ledger-based securities are, thus, equated, in many respects, to negotiable instruments and the Federal Act on Private International Law (PILA) of 18 December 1987 has

---

the Cryptocurrency Industry" (*McDermott*, 1 October 2021) <https://www.mwe.com/it/insights/a-flurry-of-cftc-actions-shock-the-cryptocurrency-industry/>.

46 Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register vom 25. September 2020, RO 2021 33. The Act to Adapt Federal Law to Developments in Distributed Ledger Technology (DLT Act) has been complemented with an Order (Verordnung zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register vom 18. Juni 2021, RO 2021 400) to introduce further amendments into Swiss financial markets law.

47 Bundesgesetz betreffend die Ergänzung des Schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht) vom 30. März 1911, SR 220 (Swiss Civil Code of Obligations).

been amended accordingly (see especially Article 145a PILA).[48] Moreover, the DLT Act has been complemented with an Order to introduce further amendments into Swiss financial markets law.[49]

Last but not least, on 8 June 2021 the government of El Salvador adopted the Ley Bitcoin and on 7 September 2021, El Salvador became the first country to make bitcoin legal tender.[50]

2.2 *Towards a Common Understanding of Cryptocurrencies*

The aforesaid attempts to frame cryptocurrencies into substantive law clearly show, firstly, that they are not treated as the cryptographic strings of characters that they in fact are, *i.e.* data or information, but rather for the notional status that they have,[51] which is based on an implicit agreement or, rather,

48 Bundesgesetz über das Internationale Privatrecht (IPRG) vom 18. Dezember 1987, SR 291.

49 Ordinanza del Consiglio federale sull'adeguamento del diritto federale agli sviluppi della tecnologia di registro distribuito del 18 giugno 2021, RO 2021 400.

50 *Cf.* Asamblea Legislativa, "El Salvador, the first country in the world to recognise Bitcoin as legal tender" (*Asamblea Legislativa*, 9 June 2021) <https://www.asamblea.gob.sv/node/11282>. While the law maintains the U.S. dollar as the national unit of account, it mandates the acceptance of Bitcoin by agents unless technical impediments exist. A new digital means of payments, *i.e.*, the e-wallet Chivo operating in both U.S. dollars and bitcoin, has been introduced and heavily supported by the government to promote financial inclusion (each qualifying citizen who downloaded the application received an endowment of USD 30). This led to protests and resulted in skepticism from economists and others. As a result, El Salvador President Nayib Bukele tweeted in August that businesses did not have to accept bitcoin. The law also guarantees the automatic conversion from bitcoin to U.S. dollars through a trust fund funded with USD 150 million from the budget, and in practice the conversion is done in Chivo. Later on, in International Monetary Fund, "Staff Concluding Statement of the 2021 Article IV Mission" (*IMF*, 22 November 2021) <https://www.imf.org/en/News/Articles/2021/11/22/mcs-el-salvador-staff-concluding-statement-of-the-2021-article-iv-mission>, the IMF concluded that "[g]iven Bitcoin's high price volatility, its use as a legal tender entails significant risks to consumer protection, financial integrity, and financial stability. Its use also gives rise to fiscal contingent liabilities. Because of those risks, Bitcoin should not be used as a legal tender. Staff recommends narrowing the scope of the Bitcoin law and urges strengthening the regulation and supervision of the new payment ecosystem. Like for other e-wallets, Chivo should be required to fully safeguard customers' funds, both in U.S. dollars and Bitcoin, by segregating and ring-fencing reserve assets. Stronger regulation and oversight of the new payment ecosystem should be immediately implemented for consumer protection, anti-money laundering and counter financing of terrorism (AML/CFT), and risk management. Banking regulation should incorporate prudential safeguards such as conservative capital and liquidity requirements related to Bitcoin exposure. Measures to limit fiscal contingent liabilities, such as winding down the trust fund or withdrawing public subsidies to Chivo, should also be promptly considered."

51 Fox (n 31), para. 6.18.

expectations, between participants to the systems where cryptocurrencies are created and transferred, that those strings actually represent a value, resulting from supply and demand balancing, and that "the consensus rules which underpin the system will be applied and will not be altered fundamentally such as to deprive each participant of the association to particular units within the system and the power to deal with those units."[52] Second, the classification of cryptocurrencies varies depending on the diverse use cases, *i.e.* store of value, tools for investment or means of payment. Third, the notional value of cryptocurrencies, their status as creatures of the law (albeit the law here is, at least at the outset, a code), and the fact that, because of the notional embodiment of the value in cryptographic strings, they represent a safe vehicle to transfer value from one person to another,[53] on one hand, might place cryptocurrencies in the realm of negotiable instruments (or even of money) and, on the other hand, those very same features, are a driver for their use as investment vehicles.

2.2.1 Cryptocurrencies as "Purely *de facto* Assets"

However, along the many discussions concerning the intrinsic nature of cryptocurrencies, there is a common understanding that cryptocurrencies, and namely bitcoins, neither represent nor give a claim against an issuer,[54] hence the classification as "purely *de facto* assets" acknowledged, for instance, in the Swiss Federal Council message accompanying the proposal for the DLT Act.[55] This, actually, seems to be the key distinctive feature of "pure" cryptocurrencies from other crypto assets, including stablecoins,[56] which may also be used and accepted as payment instruments.

---

52 Andrew Dickinson, "Cryptocurrencies and the Conflict of Laws" in David Fox and Sarah Green (eds), *Cryptocurrencies in Public and Private Law* (OUP 2019), 181–182 para. 5.107.

53 Fox (n 31), para. 6.18.

54 EBA Opinion (n 12), para. 30; Financial Conduct Authority (FCA), "Guidance on Cryptoassets (Consultation Paper CP19/3" (*FCA*, January 2019), paras. 3.35, 3.60 <https://www.fca.org.uk/publication/consultation/cp19-03.pdf> accessed 5 June 2022; Swiss Federal Council report, "Legal framework for distributed ledger technology and blockchain in Switzerland. An overview with a focus on the financial sector" (*Federal Council*, 14 December 2018), 46 para. 5.1.2.1 <https://www.newsd.admin.ch/newsd/message/attachments/55153.pdf>; Iris M. Barsan, "Legal Challenges of Initial Coin Offerings (ICO)" (2017) 3 Revue Trimestrielle de Droit Financier (RTDF) 54, 58; Fox (n 31), para. 6.30; Carr (n 30), 180–181 para. 7.07.

55 See Messaggio concernente la legge federale sull'adeguamento del diritto federale agli sviluppi della tecnologia di registro distribuito del 27 novembre 2019, FF 2020 223, 232.

56 ECB Crypto-Assets Task Force, "Stablecoins: Implications for monetary policy, financial stability, market infrastructure and payments, and banking supervision in the euro area

Notably, the recent Proposal for an EU Regulation on Markets in Crypto-assets,[57] as resulting from the latest steps of the legislative procedure, seems to have acknowledged that distinction, insofar as it provides for a differentiated treatment between e-money token, the users of which shall be granted with a claim on the issuer of such tokens, *i.e.* the right to redeem their tokens at any moment and at par value against the currency referencing those tokens, and "other crypto-asset referencing one official currency of a country" that "do not provide a claim at par with the currency they are referencing or limit the redemption period."[58] Namely, the Proposal provides for different regimes, respectively, for "asset referenced tokens" (Title III of the Proposal),[59] "electronic money tokens" (Title IV) and "crypto-assets, other than asset referenced tokens or electronic money tokens" (Title II), including, but not limited, to utility tokens.[60] Moreover, for the purpose of the Proposal, the definition of "crypto asset" refers to "a digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology,"[61] whereby "value includes external, non-intrinsic value

(Occasional Paper Series No. 247)" (*ECB*, September 2020), 8 <https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op247~fe3df92991.en.pdf> accessed 30 November 2021.

57 Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, [2020] COM/2020/593 final, 2020/0265(COD), art. 44 (hereinafter "MiCA Proposal").

58 See *Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 - Mandate for negotiations with the European Parliament (14067/21 of 19 November 2021)*, Recital 10 (hereinafter, 'Council Mandate for negotiations'), and *European Parliament Economic and Social Committee, Report on the proposal for a regulation of the European Parliament and of the Council on markets in crypto-assets and amending Directive (EU) 2019/1937 (A9-0052/2022 pf 17 March 2022)*, Recital 10 (hereinafter, 'ESC Report'). Accordingly, the EBA had previously pointed out that "the difference between electronic money and a virtual currency is that the latter is not necessarily attached to a FC [i.e., a fiat currency], *i.e.* it does not have a fixed value in a FC and, furthermore, is not necessarily fixed to be redeemed at par value by an issuer." EBA Opinion (n 12), para. 31. The view is upheld also by the Financial Conduct Authority (n 54), 31 para. 3.61.

59 According to Dirk A. Zetzsche et al., "The Markets in Crypto-Assets Regulation (MICA) and the EU Digital Finance Strategy (EBI Working Paper Series No. 2020/77)" (*SSRN*, 5 November 2020), 12 <http://dx.doi.org/10.2139/ssrn.3725395>, the proposed global stablecoin Libra would fall under this category. See *infra* (n 70).

60 Council Mandate for negotiations (n 58), Recital 9, and ESC Report (n 58), Recital 9 .

61 Council Mandate for negotiations (n 58), art. 3 para. 1(2). The Economic and Social Committee of the European Parliament has specified the notion of "digital representation" by adding the requirement that it "is in the form of a coin or a token or any other digital medium": see ESC Report (n 58), art. 3 para. 1(2).

attributed to a crypto-asset by parties concerned or market participants, meaning the value can be subjective and can be attributed only by the interest of someone purchasing the crypto-asset."[62] Therefore, despite the claim that "any definition of 'e-money tokens' should be as wide as possible to capture all the types of crypto-assets referencing one single official currency of a country" and that "strict conditions on the issuance of e-money tokens should be laid down, including the obligation for such e-money tokens to be issued either by a credit institution as defined in Regulation (EU) No 575/20138 of the European Parliament and of the Council, or by an electronic money institution authorised under Directive 2009/110/EC,"[63] "pure" cryptocurrencies seem to fall under the residual category of "other crypto assets."[64] The same Proposal envisages a more general distinction between crypto assets that may qualify as "financial instruments as defined in Article 4(1), point (15), of Directive 2014/65/EU" (*i.e.*, MiFID II Directive)[65] (or as deposits, funds, securitisation positions, insurance or pension products according to the respective relevant EU provisions,[66] which, incidentally, should be neutral as regards the use of technology),[67] and those which are not covered by those regimes and are, accordingly, included in the Proposal, with the additional aforesaid sub-distinction. With regard to pure payment-type crypto assets, however, the European Securities and Markets Authority (ESMA), in its "Advice" concerning "Initial Coin Offerings and Crypto-Assets" of 9 January 2019 held as "unlikely" that they qualify as financial instruments.[68]

62 Council Mandate for negotiations (n 58), Recital 2.

63 *Id*.

64 Also, Zetzsche et al. (n 59), 25, seem to concur with this view.

65 See Council Mandate for negotiations (n 58), art. 2 para. 2 *litt*. b and Recital 3. The Economic and Social Committee, "because of the specific features linked to their innovative and technological aspects", has recalled the need "to identify clearly the requirements for classifying a crypto-asset as a financial instrument", recommending that, for that purpose, the European Securities and Markets Authority (ESMA) is tasked by the Commission with publishing "guidelines in order to reduce legal uncertainty and guarantee a level playing field for market operators": ESC Report (n 58), Recital 2a.

66 Council Mandate for negotiations (n 58), art. 2 para. 2 *litt*. c-k and Recital 3.

67 *Id*., Recital 3.

68 European Securities and Markets Authority (ESMA), "Advice: Initial Coin Offerings and Crypto-Assets" (*ESMA*, 9 January 2019), 19 para. 80 <https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf>. *Contra* Cass pen (2), 30 November 2021 n 44337 (unpublished).

Although the opposite view, that cryptocurrencies may well embody claims, has also been sometimes maintained both with regard to bitcoins[69] and to Libra Coins,[70] recently re-nominated Diem Coins,[71] what is more relevant here is that, if a general conflict-of-laws regime for crypto assets is to be conceived, any legislative policy option (and, namely, any connecting factor) based on the idea that a claim is embedded in those assets might struggle to apply to "pure" cryptocurrencies.

However, although the aforesaid distinction might be of relevance to identify the most suitable connecting factors, it is hardly deniable that, once it is acknowledged that cryptocurrencies may be regarded as store of value – purely notional or linked to the value of a fiat currency –, and are susceptible to be transferred and traded,[72] on one hand, it may well be that exclusive rights are asserted over them and that a law regards those claims as worthy of protection against conflicting or competing interests of other parties. On the other hand, it is also hardly deniable that the transfers of cryptocurrencies which take place through the blockchain represent the implementation of a transaction of whichever nature.

Overall, the definition of cryptocurrencies as purely *de facto* assets – that do not incorporate, nor represent, claims, but because of their (notional) value may be the object of transactions – seems sufficient to call for a specific conflict-of-laws analysis.

2.2.2 The Knowledge of the Private Key as (the Only) Basis for Control over Cryptocurrencies

In at least apparent contrast to the above, with a view to reconciling the autonomy and immutability of blockchain transfers with the requirement of private justice, a very thorough theory has been recently developed according to which, since the power of the holder of bitcoins resides in his/her knowledge

69 *Cf.* Kelvin F.K. Low, "Bitcoins as Property: Welcome Clarity?" (2020) 136 Law Quarterly Review 345, criticising the court's findings in *AA* (n 33) that bitcoins are an intangible property but not a chose in action.

70 Antoine d'Ornano, "Sur le projet Libra" (2020) Revue critique de droit international privé, 179 ff. The description of the original features of the Libra system and coins may be found in the historical White Paper at <https://www.diem.com/en-us/white-paper/> accessed 30 November 2021.

71 See the website of the Diem Association, "Welcome to the Diem project" (*Diem Association*) <https://www.diem.com/en-us/> accessed 5 June 2022, whereby the whole system seems still under development.

72 Matteo Solinas, "Investors' Rights in (Crypto) Custodial Holdings: *Ruscoe v Cryptopia Ltd* (*in Liquidation*)" (2020) 81 Modern Law Review 155, 160.

of the private key (that allows him to initiate the transfer to the address, *i.e.*, the public key, of the recipient),[73] one should accept the record on the blockchain as a fact that reveals the current holder of the bitcoin and creates a legal presumption of him being the legitimate holder of that crypto asset (unless it can be proven that the crypto asset has been obtained illegally).[74] Therefore, the law should regard that transfer as immutable and "substitute a conceptualization of the transfer in terms of property law by an analysis that is based on remedies under the law of obligations."[75] Accordingly, in case of mistakes or *exceptio inadimplendi*, the transferor should rely on the "reverse transfer," *i.e.* on the possibility for the law to impose an obligation on the recipient of the crypto asset to return it, whilst, exceptionally, in cases of hacking, blackmail or fraud the transaction could be invalidated.[76] It might be, further, worth

73 In the Bitcoin system, users are represented by addresses, which can be regarded as being like a bank account number. An example of a Bitcoin address is a string of letters and numbers (*e.g.*, 3PtFPuXZxS1CBHdG2E5EeU6FcFqGGmzepF). In this way, Bitcoin accounts are pseudonymous. Addresses are created using public key cryptography. The owner of the address is the holder of the private key that corresponds to the public key that has been used to create the address. Therefore, the private key is the proof that a specific address belongs to this user. As a result, private keys must be protected, as their loss means loss of proof that this address belongs to the user and, as a direct consequence, the inability to use the bitcoins in the corresponding accounts. As Bitcoin is not controlled by an entity, it is impossible to claim missing private keys. Addresses are used to hold bitcoins; a user is usually the holder of many addresses. There is no limit on how many addresses a user can have; rather, it is advised to use a new address when receiving bitcoins rather than reusing addresses. This makes the tracking of addresses and linking them to the owners more difficult. To perform a transaction – for example, Alice wants to send 20 bitcoins (BTC) to Bob – Alice will have to prove that she is the owner of an account or a number of accounts that hold at least 20 BTCs. She does this by digitally signing the transaction with the private keys of these accounts. Once signed, rather than being sent directly to Bob, the transaction is broadcast on the whole Bitcoin network. Alice's transaction is pending until a special entity in Bitcoin, known as a "miner," verifies it. The miners collect pending transactions, then confirm their correctness before verifying them. To summarise, Alice wants to send 20 BTC to Bob. The closest sum of her addresses to the targeted amount is 21.1 BTC. The transaction is broadcast on the Bitcoin network and once verified, Bob receives the 20 BTC, the miner receives 0.1 BTC as a transaction fee, and 1 BTC is returned to Alice as change. Once the transactions have been verified, they are stored in a tamper-resistant and shared data structure comprising of a list of blocks which are chained together, known as a blockchain. New transactions are inserted into a block at the end of the chain and linked to the previous block of transactions, as each block references the previous block's hash.

74 Matthias Lehmann, "Who Owns Bitcoin? Private Law Facing the Blockchain," (2019) 21 Minnesota Journal of Law, Science & Technology 93, 119–120.

75 *Id.*, 123.

76 *Id.*, 128–130.

considering that, according to that theory, the factual position – *i.e.* the knowledge or, otherwise said, the possession – of the private key is seen as legally protected by way of the applicable tort, contract or security law.[77]

No matter how sound and effective the aforesaid approach may be, given the intrinsically cross-border nature of DLT, enacting the premise of such an approach – namely, the aforesaid legal presumption – would entail the general acceptance, either through the adoption of a single international instrument providing for uniform substantive rules or via parallel pieces of national legislation, that what results from the blockchain deserves, with few exceptions, to be upheld and protected by the law. For the moment, however, the abovementioned first stance taken by national lawmakers and case-law seems rather inclined to frame bitcoins into more traditional patterns of property law.

Be that as it may, the aforesaid theory has (also) the merit of drawing attention to the *de facto* situation connected with the knowledge of the private key. In the same vein, the UNIDROIT Working Group on Digital Assets and Private Law, while elaborating a set of Principles to support States in adopting substantive and conflict-of-laws rules on digital assets, has identified that situation with the term "control" and clarified that "a person has 'control' of a digital asset if: (a) …the digital asset or the relevant protocol or system confers on the person: (i) the exclusive ability to change the control of the digital asset to another person (a change of control); (ii) the exclusive ability to prevent others from obtaining substantially all of the benefit from the digital asset; and (iii) the ability to obtain substantially all the benefit from the digital asset; and (b) the digital asset or its associated records allows the person to identify itself as having" those abilities. What is more relevant here is, first, that, according to the draft Commentary to those draft Principles, the "'control' assumes a role that is a functional equivalent to that of 'possession' of movables," insofar as in the markets for digital assets, those who acquire control over the assets "expect and believe" that they have obtained, through control, the relevant exclusive abilities, and, second, that, for the purpose of the identification requirement set forth under (b), an identifying number, a cryptographic key, an office, or an account number may be of relevance, "even if the identification does not indicate the name or identity of the person to be identified."[78] Moreover, the relevance of the "exclusive ability" requirements for the purpose of said

77 *Id.*, 128.

78 Unidroit Working Group on Digital Asset and Private Law, "Issues Paper (UNIDROIT 2021 Study LXXXII-W.G.4 – Doc. 2)" (*UNIDROIT*, October 2021), 38–39 <https://www.unidroit.org/work-in-progress/digital-assets-and-private-law/#1622753957479-e442fd67-036d> accessed 30 November 2021.

Principles as "an inherent aspect of proprietary rights" acknowledges the tendency to frame the relationship between users and digital assets in terms of property rights.[79]

Therefore, the following section will address the PIL regime of cryptocurrencies, considering first their function of payment instruments and, second, their (possible, though uncertain) role as store of value. Whilst the former perspective seems relatively smooth and will be (briefly) addressed against the backdrop of the existing PIL rules concerning payment obligations, the latter is far more complicated and suggests that the tentative answers that will be offered are further tested in business scenarios.

3 The PIL Regime of Cryptocurrencies as Payment Instruments

In principle, as long as cryptocurrencies do not amount to legal tender in a country, their use as means of payment is dependent upon the will of parties, since it is for them, mainly, to accept a payment, for instance, in bitcoins, as a way of performing an obligation to pay the consideration for a good or service, subject, of course, to any relevant mandatory provision established under the law governing the contractual (or even non-contractual) obligation in question.[80] It might, indeed, be the case that the *lex contractus* mandatorily requires that any payment is delivered in a fiat currency; if so, the creditor may reject an offer to pay in any different way; otherwise parties may agree on a payment in bitcoins or something else.[81] Moreover, the *lex contractus* will be of relevance to determine whether a consideration agreed in form of cryptocurrencies, in lieu of a fiat currency, transmutes the contract into a different type, *e.g.*, a sale of goods into a barter,[82] as well as that law will govern the effects (if any) of a depreciation (or appreciation) of the cryptocurrency and the possibility for the parties to protect themselves against any fluctuation by

79 *Id.*, 39.

80 Paolo Bertoli, "Virtual Currencies and Private International Law" (2018) 54 Rivista di diritto internazionale privato e processuale 583, 599. It seems rather difficult to figure out how the principle of nominalism embodied in the *lex monetae* principle could apply to cryptocurrencies.

81 Mathias Audit, "Le droit international privé confronté à la blockchain" (2020) Revue critique de droit international privé 669, para. II.A.

82 The question is discussed against the background of English and Scot Law in the paper of the Financial Markets Law Committee (n 20), 8. See also Sarah Green, "It's Virtually Money," in David Fox and Sarah Green (eds), *Cryptocurrencies in Public and Private Law* (OUP 2019), 28–29 para. 2.42.

means of specific agreements.[83] Additionally, in case of non-performance of the payment in bitcoins, it will be for that law to establish to what extent and upon which conditions the obligation in question may be discharged through a payment in a fiat currency, as well as any other consequence, also in terms of interests or damage, connected with the nonperformance.[84] On the other hand, in relation to the manner of performance and the steps to be taken in the event of defective performance, regard shall also be had to the law of the country in which performance takes place,[85] whereby a creditor might be entitled to reject a payment in a currency other than local fiat currency, such as a cryptocurrency.[86]

Additionally, in providing for an obligation to be delivered in cryptocurrencies, parties shall take into account the possibility that overriding mandatory provisions of the law of the (foreseeable) forum ban the use of cryptocurrencies as instrument of payment, or qualify, as unlawful, a contract involving cryptocurrencies, either *per se* or because in breach of anti-money laundering or anti-terrorism regulations, or, even, of unilateral or multilateral economic sanctions. Moreover, also similar overriding mandatory provisions of the law of the country where the obligations arising out of the contract have to be or have been performed may come to be relevant for the same purpose, "in so far as those provisions render the performance of the contract unlawful" and having regard "to their nature and purpose and to the consequences of their application or non-application."[87] With regard to payment in cryptocurrencies, it should be, however, noted that the effectiveness of said provisions run the risk of being seriously impaired, both by virtue of the possibility for the parties to agree on a place of payment where those provisions are not applicable, and because of the practical difficulty in identifying the actual place of payment in DLT's settings.

83 *Cf.* Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), [2008] OJ L177/6, art. 12 para. 1 *litt.* d (hereinafter "Rome I"), and Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II), [2007] OJ L199/40, art. 15 *litt.* H (hereinafter "Rome II"). See Lord Collins of Mapesbury and Jonathan Harris (eds), *Dicey, Morris & Collins on the Conflict of Laws* (15th edn, London: Sweet & Maxwell 2012), Rule 261.

84 Richard Plender and Michael Wilderspin, *The European Private International Law of Obligations* (4th edn, Sweet & Maxwell 2015), paras. 14-030–14-032.

85 *Cf.* Rome I (n 83), art. 12 para. 2.

86 Audit (n 81).

87 *Cf.* Rome I (n 83), art. 9. See esp. Charles Proctor, Caroline Kleiner, and Florian Mohs, *Mann on the Legal Aspect of Money* (7th edn, OUP 2012), paras. 4-24-4.29.

4 ...and as "Property"

Turning to the role played by cryptocurrencies as a store of value, according to the traditional pattern in property matters, it is for the law governing property rights, as determined through the relevant conflict-of-laws provision – in principle the *lex situs* –, to establish whether a specific "thing" can be the subject matter of property rights, the classification of that thing as immovable or movable (or else), as well as the types and contents of those rights, *i.e.* the prerogatives of the person who "holds" the thing. When it comes to intangible assets, and especially, digital assets, however, the effectiveness of such a paradigm is largely put to the test, first and foremost, due to the difficulty, or rather impossibility, to identify a physical location for them, though not only because of that objective issue. Conversely, with regard to intangible assets incorporating claims, the further specificities, both in terms of notion of property rights and of applicable connecting factors, lie in the fact that the asset *is* the relationship with the debtor, which has its own governing law.

Once it is generally accepted that the factual relationship between a cryptocurrency and its holder entails that the latter has the exclusive ability to dispose of the former and to exclude others from the benefits thereof and that accordingly such relationship may be construed as property, the applicable law will determine the conditions upon which a person has a proprietary right in a cryptocurrency and that right may be validly transferred,[88] including the rules for the original acquisition of title (*e.g.* the possibility to invoke the defences of good faith purchase for value)[89] and the derivative transfer of title (generally, either through party's consent or delivery of the asset), as well as any requirements regarding time of perfection, publicity,[90] need for specification,[91] and the realisation of the right over the asset,[92] both having regard to the rights as between the transferor and the transferee *inter se*, and to the legal consequences of the transfer *vis-à-vis* third parties,[93] including the transferor's creditors.[94] As unlikely as it might seem because of the validation mechanisms

88 Lehmann (n 11), 150.

89 Fox (n 31), para. 6.57 ff.

90 Carr (n 30), paras. 7.18–7.20.

91 *Id.*, paras. 7.16–7.17.

92 Financial Markets Law Committee, "Distributed Ledger Technology and Governing Law: Issues of Legal Uncertainty" (*FMLC*, March 2018), 11 para. 4.7 <http://fmlc.org/wp-content/uploads/2018/05/dlt_paper.pdf> accessed 30 November 2021.

93 Unidroit Working Group on Digital Asset and Private Law (n 78), 41, 43–44.

94 Council of the European Union, "Proposal for a Regulation of the European Parliament and of the Council on the law applicable to the third-party effects of assignments of claims -

embedded in the blockchain systems, which are precisely aimed at preventing any double transfer of the same token, the same law will govern the priority of the rights among competing transferees of the same token. Moreover, the same law will establish the forms of security that may be validly granted over the cryptocurrency.[95]

It is now time to explore some policy options for a conflict-of-laws regime for said property aspects of cryptocurrencies.

First and foremost, among the solutions that have been so far envisaged by scholars and think-tanks for crypto assets, the approach which favours the application of the law under which the right/claim represented by the crypto asset, as admitted by its own promoters,[96] cannot apply to intrinsic tokens, such as "pure" cryptocurrencies. In fact, as anticipated, cryptocurrencies do not represent nor incorporate rights.[97] The same goes for any approach centered around the issuer of the crypto assets, since cryptocurrencies do not embed a claim against an issuer, whereas the original coder does not undertake any obligation towards the subsequent transferees of the assets.[98]

The absence of any underlying claim, coupled with the inherent nature of "pure" cryptocurrencies as items representing value, albeit a notional and volatile one, would, thus, locate their conflict-of laws regime into the realm of the *lex rei sitae* principle. This is premised (also) on the need for "an objective and easily ascertainable connecting factor to which third parties might reasonably

---

General approach (9050/21)" (*CEU,* 28 May 2021), art 5 *litt*. c <https://data.consilium.europa.eu/doc/document/ST-9050-2021-INIT/en/pdf>.

95 UK Jurisdiction Taskforce (n 33), 25; ISDA, McCann FitsGerald, and r3, "Private International Law Aspects of Smart Derivatives Contracts Utilizing Distributed Ledger Technology: Irish Law" (*ISDA*, October 2020), 29 <https://www.isda.org/a/ACrTE/Private-International-Law-Aspects-of-Smart-Contracts-Utilizing-Distributed-Ledger-Technology-Irish-Law.pdf> accessed 30 November 2021.

96 Koji Takahashi, "Blockchain-based Negotiable Instruments (with Particular Reference to Bills of Lading and Investment Securities)" (*SSRN*, 6 October 2021), para. 5.6.3 <https://ssrn.com/abstract=3937664>.

97 Financial Markets Law Committee (n 92), 20 para. 6.27; Michael Ng, "Choice of law for property issues regarding Bitcoin under English law" (2019) 15 Journal of Private International Law 315.

98 European Parliament resolution of 8 October 2020 (n 3), Recital AN; Filippo Annunziata, "Speak, If You Can: What Are You? An Alternative Approach to the Qualification of Tokens and Initial Coin Offering" (2020) 17 European Company and Financial Law Review 129, 150–53; ISDA. Jones Day, and r3, "Private International Law Aspects of Smart Derivatives Contracts Utilizing Distributed Ledger Technology: French Law" (*ISDA*, October 2020), 19 <https://www.isda.org/a/ZCrTE/Private-International-Law-Aspects-of-Smart-Derivatives-Contracts-Utilizing-DLT-French-Law.pdf> accessed 30 November 2021.

look to ascertain questions of title," which represents the first component of the rationale underlying the application of that principle in property matters[99] and is even more relevant for assets that could be used by companies to obtain liquidity and have access to credit through collateralisation.[100]

However, the aforementioned technical features of cryptocurrencies, which originate in and are transferred through a ledger system that is dematerialised and distributed, make the application of the situs principle, at least in its traditional form, impossible in practice and unsuitable for the second limb of its rationale, which lies in the fact that "the country of the *situs* has control over the property and a judgment in conflict with the *lex situs* will often be ineffective,"[101] since the actual possibility for an authority to have any form of control over crypto assets, including to enforce any regulation, should rely on different grounds. Nevertheless, both limbs of that rationale should be included in the parameters against which to test the soundness of any conflict-of-laws regime for cryptocurrencies too, besides those related to the foreseeable use-cases of those assets.

In that regard, the need to find appropriate PIL solutions is reinforced by the pattern of disintermediation that is (or should be) intrinsic to DLT ecosystems by virtue of the traceability and collective validation of transactions taking place in and through those ecosystems. Disintermediation should *per se* rule out the possibility to envisage conflict-of-laws rules modelled on the ones related to book-entry securities that are based on the location of the relevant intermediary. Nevertheless, the current practice reveals that the prevailing framework for cryptocurrencies has become an indirect holding pattern, characterised by a combination of two-tier networks based on a distributed and decentralised scheme where the nodes are often represented by exchanges, *i.e.* crypto asset service providers in the language of the proposed EU Regulation on Markets in Crypto-assets,[102] that are connected to the adjacent nodes within the blockchain (*i.e.* a distributed network) and where additional nodes are also formed among investors in cryptocurrencies at the level of the relevant exchanges (*i.e.* a decentralised network).[103] Such practice may neither affect the technical features of the cryptocurrencies' holding and transfer schemes, as far

99 Lord Collins of Mapesbury and Jonathan Harris (n 83), para. 22-025.

100 Proposal for a Regulation of the European Parliament and of the Council on the law applicable to the third-party effects of assignments of claims, [2018] COM(2018) 96 final, 2018/044 (COD), 2.

101 Lord Collins of Mapesbury and Jonathan Harris (n 83), para. 22-025.

102 MiCA Proposal (n 58), art. 3 para. 1 n 9.

103 Solinas (n 72), 156.

as the exchanges/intermediaries' holding pattern applies the same schemes, nor, accordingly, the need to have legislative solutions well aligned with technology, but may have relevance when testing any legislative option against the substantive interests and aptitudes of the end-users, In fact, it might turn out that more often than expected, DLT end-users are professional operators.

Furthermore, a basic theoretical question (with relevant practical consequences) should be considered. Conceptualising the relationship between persons and cryptocurrencies in terms of property rights entails a generalised acceptance of the preliminary proposition(s) that (i) a notional value is worthy of being regarded as the subject matter of property rights, and (ii) the transfer of that value, *i.e.* the cryptocurrencies, according to the technical requirements of DLTs, implies a transfer of property right(s) over that value or, in other words, that a transfer of cryptocurrencies through the system is a legally sound way to dispose of said assets. However, this second proposition does not necessarily mean that a "transfer" within the system from which cryptocurrencies derive their existence is the only way to "dispose of" property rights over the same, unless a law establishes that it is so in terms of conditions for the validity of the transfer and opposability of the same against third parties. The last question is particularly relevant when it comes to investigating desirable conflict-of-laws approaches (and, particularly, about connecting factors) and the (possible) need to take into account both on-chain and off-chain acts of disposition for that purpose. In that regard, the business practice may, of course, offer some very much useful data to construct some answers, but the final say rests with the relevant applicable law, …which leads to a kind of circular argument.

However, as advanced above,[104] an alternative theory has suggested that the proposition under (i) is replaced by a "protection by private law" that goes "beyond traditional conceptions of property in physical objects" and is "independent of any showing of legal title," whereby "the mere factual situation that the private key was created for some person should suffice as a basis for claim of return"[105] and for the recognition of "some form of legal status" that is "also necessary for the creation of a security right over the crypto asset" in question. The same doctrine has further argued that it could be left "to the applicable tort, contract, or security law" to "call" that status as "property" or

104 *Supra* para **2.2.2.**
105 Lehmann (n 74), 128.

"possession" or "by another term,"[106] as well as to protect it through the relevant remedy.[107]

In-between stands, so to say, a third approach, which does not give up on characterising cryptocurrencies – or, rather, the "factual" benefit accruing to a person as a participant to a cryptocurrency system (the value of which relies upon "a legitimate expectation, founded on the technological features of the system, that the consensus rules which underpin the system will be applied and will not be altered fundamentally such as to deprive each participant of the association to particular units within the system") – as "a form of intangible property within the conflict-of-laws."[108] Yet, a distinction is made between "internal effects" of transactions within a cryptocurrencies system, which should be resolved by reference to the system's consensus rules and any law applicable by virtue of the relevant conflict-of-laws rules concerning contractual obligations,[109] on one hand, and the "external effects," to which separate choice of law rules apply, on the other. At the same time, however, this doctrine admits that the proprietary character of a cryptocurrency "depends" on relationships within the system,[110] illustrating that proposition through the case of parties wishing to create a security interest over units of a cryptocurrency. To this end, said parties may, or may not, enter into an arrangement which involves a transaction within the blockchain initiated by the grantor for the benefit of the grantee. In the second scenario the creation of the security may entail, for instance, that the grantor gives the grantee control over or access to a cryptocurrency wallet. In the first scenario, instead, the initiation of a transaction within the DLT system would engage "the separate relationships of the grantor, grantee, and many others as participants in the system."[111] By way of further example, it is mentioned that, if, for some technical reasons, the transaction within the system is ineffective, the grantee may need to rely on a proprietary entitlement existing outside the system. Also, if the transaction within the system is successfully validated but the system lacks the technical possibility to re-vest the cryptocurrency in the grantor upon redemption, the

106 *Id.*, 127–128.

107 For a similar critique of the adoption of the "Physical Model" to frame the relationship between persons and intangible assets in the wake of the advent of the electronic era see Joanna Benjamin, *Interests in Securities: A Proprietary Law Analysis of the International Securities Markets* (Oxford: OUP 2000), 303 ff.

108 Dickinson (n 52), 127 para. 5.97.

109 *Id.*, 106 ff.

110 *Id.*, 127 para. 5.95.

111 *Id.*, 127 para. 5.94.

grantor may benefit from the protection afforded by the "external" proprietary entitlement. By the way, the aforesaid examples seem to provide support to the conceptualisation of cryptocurrencies holding pattern in terms of property rights, while, at the same time, demonstrating the relevance of and the need for "external" legal remedies to enforce those rights.

5 Available Options for a Conflict-of-Laws Regime

In going over the various possible approaches to determine the law applicable to "pure" cryptocurrencies, first, certain objective connecting factors that are pegged to the ecosystem in which cryptocurrencies originate and are transferred will be considered, then, some propositions centered around the transferor and/or the transferee will be addressed, and, finally, schemes based on party autonomy will be explored.

5.1 *The "PROPA" and "PREMA" Criteria*

A first batch of proposals looks to the place of the relevant operating authority or administrator ("PROPA"),[112] either in form of objective connecting factor or by empowering that authority to establish the applicable law. The significance of that connection would be, of course, particularly relevant in case of an operator which is registered and supervised under some national law.[113] Both versions, indeed, reflect the wish for a single law to govern all aspects of transactions within the system.[114] Such an approach presupposes that the relevant DLT system is permissioned and not decentralised,[115] with a single entity performing core functions, such as management activities, and acting as a point of contact and a gatekeeper on behalf of the regulators. Moreover, the enactment of a rule grounded on PROPA would, in any case, require a clarification of the

112 In the opinion of the UK Jurisdiction Taskforce (n 33), 99, in determining whether English and Welsh law governs the proprietary aspects of dealings in crypto assets, one of the factors that might be "particularly relevant" is whether there is any centralised control in England and Wales.

113 Lehmann (n 11), 169.

114 Maisie Ooi, "Choice of Law in the Shifting Sands of Securities Trading," in Andrew Dickinson and Edwin Peel (eds), *A Conflict of Laws Companion. Essays in Honour of Adrian Briggs* (Oxford: OUP 2021), 213.

115 Hubert de Vauplane, "Blockchain And Conflict of Laws" (2017) Revue Trimestrielle de Droit Financier, 52.

actual role of the "relevant administrator," by specifying the activities which represent the essence of that role and a threshold of "relevance," especially in cases where the entity in question only performs limited functions, such as providing technical access to the system, or where there are two (or more) entities performing similar functions located in different states.[116] However, PROPA seems unable to work for permissionless/public systems like Bitcoin.

The same rationale would underlie an approach based on the location of the original coder of the DLT system or the private master key for the same (usually the primary residence of the keyholder; hence the acronym "PREMA"), that is the key by which the relevant operator or administrator is enabled to control all transfer of assets within the system, in that such master key is used to encrypt and store all other keys in the system. In either case, besides the costs to market participants of ascertaining the location of these entities, one may question why the original coder should affect the ongoing life of the system (and all the transactions therein executed), especially where (s)he is not also the system administrator.

5.2 *The Transferor's or the Transferee's Location*

A second group of theories looks to the location of the parties to the transactions, either in the form of their habitual residence (or centre of main interest or domicile) or of their private encryption key (or of the wallet where private keys are stored).[117]

The solutions based on the transferor mirror the approach undertaken in the latest available text of the Proposal for Regulation on the law applicable to third party effects of assignment of claims (*per se* not applicable to the

116 Financial Markets Law Committee (n 20), 18 paras. 6.16–6.17.

117 This approach is supported by de Vauplane (n 115), 50 and Sarah Green and Ferdisha Snagg, "Intermediated Securities and Distributed Ledger Technology," in Louise Gullifer and Jennifer Payne (eds), *Intermediation and Beyond* (Oxford: Hart 2019), 357, based on the analogy with traditional bearer securities. The UK Jurisdiction Taskforce (n 33), 99, qualifies as "particularly relevant" also "whether a particular crypto asset is controlled by particular participant in England and Wales because, for example, a private key is stored here."

third party effects of the transfer of crypto assets)[118] as a general rule.[119] In both frameworks, the main advantage of said criterion has been identified in the convenience it brings to the transfer of claims/assets in bulk, in that all the claims/assets held by the transferor-assignor-borrower become subject to the same law with regard to third party effect of the transfer-assignment.[120] Moreover, that criterion offers the additional advantage that it does not put the transferee-financier in a more favourable position than other possible competing claimants seeking to challenge the transfer.

On the other hand, the solutions based on the location of the transferee (or of her private key) mirror the PRIMA principle embodied in the FCD[121] and, with certain differences, in the Hague Securities Convention,[122] where the relevant factor is also in the control of the transferee, *i.e.* the financier, who, therefore, is allowed to ascertain the applicable law much more easily and before anyone else. The main advantage of the transferee/current holder rule has been identified in that it applies the law of the state which can effectively enforce any judgment.[123]

However, against approaches based on the transferor's or transferee's location the following critiques have been raised: the blockchain becomes subject to as many laws as the number of states where the users or their private keys

118 Council of the European Union (n 94), art. 1 para. 1ab. Conversely, pursuant to art. 4 para. 2 of the same Proposal, "[t]he law applicable to the assigned claim shall govern the third-party effects of the assignment of: … (ba) claims arising out of crypto-assets that do not qualify as financial instruments or electronic money." See also Recital 16bis and Recital 27bis. According to Recital 16bis, last sentence, "[i]n order to avoid characterisation problems as to whether a certain crypto-asset qualifies as a financial instrument or another type of crypto-asset, claims arising from all crypto-assets should be covered by th[e] Regulation, with the exception of claims arising out of crypto-assets that qualify as transferable securities, money-market instruments or units in a collective investment undertaking." That provision will, of course, apply to all crypto assets capable of giving rise to "claims" according to the definition provided in art. 2 *litt*. d, *i.e.*, "the right to claim a debt of whatever nature, whether monetary or non- monetary, and whether arising out of a contractual or a non-contractual obligation." It is worth noting that art. 2 *litt*. hc and Recital 16bis of the Proposal expressly refer to the definition of "crypto-asset" "as defined" in the relevant provision of the MiCa Proposal (n 58).

119 Council of the European Union (n 94), art. 4 para. 1.

120 Ooi (n 114), 216.

121 Directive 2002/47/EC of the European Parliament and of the Council of 6 June 2002 on financial collateral arrangements, [2002] OJ L168/43, art. 9.

122 Hague Conference on Private International Law, "Convention of 5 July 2006 on the Law Applicable to Certain Rights in Respect of Securities held with an Intermediary" (*HCCH*, 5 July 2006), art. 4 <https://www.hcch.net/en/instruments/conventions/full-text/?cid=72>.

123 Ng (n 97), 335.

are located, the identity of users is often unknown (or difficult to trace) and, accordingly, it is difficult to identify the place of the private key.[124] Moreover, the private key is a code that may or may not be associated with any particular tangible device which generates it or stores it.[125] An additional significant disadvantage of the criteria based on the transferor's location would be that they would often provide unclear answer to questions of entitlement in cases of joint transferors or a change in the transferor's habitual residence or domicile.[126]

The same objections have been raised against another doctrine, likewise centered on the transferor's location. In fact, building upon the analogy between the factual benefit accruing to a person as participant in the blockchain and the goodwill of a business, which in English conflict of laws is equally qualified as a species of intangible property, it is argued that "proprietary effects outside the cryptocurrency system of a transaction relating to cryptocurrency shall in general be governed by the law of the country where the participant resides or carries on business at the relevant time."[127] In case that the relevant user resides or carries on business in more than one state at that time, the relevant place would be the place of residence or business of the user "with which the participation [in the cryptocurrency] that is the object of the transaction is most closely connected."[128] The emphasis on the effects of transactions outside the cryptocurrencies system, on one hand, allows that doctrine to highlight the predictability and ease of application in comparison with other possible choice of law approaches, as well as the close alignment with the rules

124 Audit (n 81), para. I.B; Ooi (n 114), 215.

125 Ooi (n 114), 215.

126 Financial Markets Law Committee, (n 20), 20 para. 6.22.

127 This approach has been applied in *Ion Science & Duncan Johns* (n 34), 13, whereby, as reported by Lorna Sleave (n 34), English law was found to apply, as England was the place where the damage occurred. This was on the basis that Mr. Johns' bank account was an English account, or that the funds were taken from the applicants' control in England, because either Mr. Johns' computer was in England, or because the relevant bitcoin was located in England prior to the transfer. As to the latter point, this was said to be because the *lex situs* of a crypto asset is the place where the person or company who owns it is domiciled, although Mr. Justice Butcher acknowledged there is no decided case on this point and relied on textbook authorities (which, incidentally, has been identified with Andrew Dickinson in the following online posting: Andrew Moir et al., "High Court considers where cryptocurrencies are located and compels disclosure of information by cryptocurrency exchanges outside the UK" (*Herbert Smith Freehills*, 24 February 2021) <https://hsfnotes.com/litigation/2021/02/24/high-court-considers-where-cryptocurrencies-are-located-and-compels-disclosure-of-information-by-cryptocurrency-exchanges-outside-the-uk/>.

128 Dickinson (n 52), 132 para. 5.109.

that apply to cross-border insolvency.[129] On the other hand, the distinction between the external effects, governed by the law of the state of the transferor's residence or business, and the internal effects, tentatively attributed by this doctrine to the law governing the (contractual) relationship between participants in the system, would allow the assertion of proprietary rights based on the law applicable to "external effects" against another user who, after being granted "externally" with security interests in a cryptocurrency, uses the information provided to him by the owner of the cryptocurrency (and grantor of the security interest) to initiate an irreversible transaction within the system in favour of a third party. One may reply that distinguishing between external and internal proprietary effects for the purpose of identifying the applicable law creates exposure to misalignments, for instance, in the substantive requirements for the opposability of property rights, thereby paving the way for inextricable conflicts of competing assertions of proprietary rights on the part of different persons. While advocating for uniform substantive rules, especially on this aspect, one should not overrate the actual impact of such misalignments, keeping in mind that the existence of different proprietary rights, each governed by a different law, is a very common pattern in the framework of proprietary rights over intermediated securities.[130] Yet, an additional warning is to be given about the need to have in place some kind of settlement regime, capable of (i) combining coherently both the external and the internal proprietary effects of transactions over cryptocurrencies, and (ii) counterbalancing the lack of deterministic operational finality of said transactions[131] with legal mechanisms to define the moment(s) of settlement finality.[132]

---

129 *Id*., 132–133 para. 5.110.

130 See Victoria Dixon, "The Legal Nature of Intermediated Securities: An Insurmountable obstacle to Legal Certainty?," in Louise Gullifer and Jennifer Payne (eds), *Intermediation and Beyond* (Oxford: Hart 2019), 70 ff, for a detailed analysis of that pattern in cross-border settings.

131 The finality of payments and settlements on the Bitcoin blockchain is viewed as probabilistic due to the likelihood that the most recent transactions embedded in the blockchain may be undone or bitcoins may be double spent due to a formation of a fork: see Bank for International Settlements, "Annual Economic Report" (*BIS*, June 2018), 101–104 <https://www.bis.org/publ/arpdf/ar2018e.htm> accessed 22 February 2022. However, the same applies to the operational settlement with cash and any other means of electronic payments, as there is always a theoretical possibility of taking the cash back by using brute force or reversing the transaction due to a technical failure in the payment system, including that of a central bank.

132 The need for (and the difficulties linked to) the establishment of a regime capable of providing legal finality in Proof-of-Work blockchains are pointed out by Hossein Nabilou, "Probabilistic Settlement Finality in Proof-of-Work Blockchains: Legal Considerations" (*SSRN*, 31 January 2022) <http://dx.doi.org/10.2139/ssrn.4022676>. On this topic see

5.3 *The Elective Situs/Lex Creationis Approach…*

The intrinsic connection between "pure" cryptocurrencies and the system in which they originate and through which they are transferred is, instead, at the core of the approach which looks to the law governing the system, alternatively, as the "*situs*" of the assets or the *lex creationis*, *i.e.* the law of the system by which cryptocurrencies are created.[133] In either case, the law applicable to the system is identified with the law agreed to by participants to the system (the originator and the nodes) either explicitly or implicitly by dealing with crypto assets within the system.[134] The advantages of this approach, sometimes referred to as the "elective situs" following the model of the "contractual PRIMA" which labels the Hague Securities Convention, is said to lie in the fact that the effects of all the transactions within the system are governed by the same law and that participants in the system cannot complain about the application of that law since it is the law to which they have submitted, which, moreover, has the most significant connection with the crypto assets, and especially native tokens. Moreover, the law governing the system is said to be easily ascertainable both by parties to each transaction, as well as by third parties, themselves likely to be participant in the same system. The main obstacles to the elective *situs/lex creationis* approach lie, on one hand, in the possible reluctance to see the effects of a choice-of-law agreement extended to third parties who do not participate in the relevant system, and, on the other hand, in possible concerns regarding the risk of circumvention of regulatory requirements or related to the choice of a law which might be subject to undue external or private influence. The latter concerns could, however, be addressed by combining the elective *situs* rule with a requirement that the selected law has an objective connection with the system, which could, moreover, be specified through a list of factual elements which should be considered for that purpose. Alternatively, the effectiveness of the choice-of-law agreement could be made conditional upon the approval of the relevant regulatory authority (which would entail, however, the need for the relevant legislative forum to be entitled to adopt both conflict-of-laws and regulatory rules within the same national or international framework). It

---

also Committee on Payments and Market Infrastructures, "Distributed ledger technology in payment, clearing and settlement: An analytical framework" (*BIS*, February 2017) <https://www.bis.org/cpmi/publ/d157.pdf> accessed 22 February 2022; Advisory Groups on Market Infrastructures for Securities and Collateral and for Payments, "The use of DLT in post-trade processes" (*ECB*, April 2021) <https://www.ecb.europa.eu/pub/pdf/other/ecb.20210412_useofdltposttradeprocesses~958e3af1c8.en.pdf?2779d0668b55434a0e67174b3f1183a4> accessed 22 February 2022.

133 Ooi (n 114), 220–221.

134 *Id.*, 219.

might be worth noticing, however, that the Council Mandate for negotiations regarding the MiCA Proposal provides that the crypto-asset white paper which, according to Article 4 para 1 litt. b, shall accompany a request for admission of a crypto asset to trading on a trading platform for crypto assets, shall contain, on one hand "the applicable law and the competent court of the offer and of the crypto-asset" (Art. 5 para 1 litt. h), and on the other, "…the following clear and prominent statement on the first page: 'This crypto-asset white paper has not been reviewed or approved by any competent authority in any Member State of the European Union…'" (art 5 para 3).

5.4 *…with Some Addenda*

However, what the elective *situs* approach fails to provide is a solution for systems (or assets) which lack any agreement as to the applicable law, and this might often be the case for permissionless systems. A comprehensive conflict-of-laws regime for proprietary effects of transactions over cryptocurrencies, based on the elective *situs* and some requirements in terms of objective connection of the selected law, therefore requires a fall-back rule,[135] which should provide different sub-rules for permissioned and permissionless systems. As for the former, the PROPA approach might be a workable solution which, like the main rule, would lead to a single law applicable to the effects of all transactions within the system. For the latter systems, the reasons for having a single law applicable to all transactions seem much weaker and, in any case, it would be very complicated to achieve this goal in light of the aforesaid difficulty to identify a meaningful objective connecting factor for permissionless systems. For those systems, the transferor's habitual residence or registered seat might represent a practical solution, at least for the effects of transaction in cryptocurrencies outside the system, whereby in most cases it should be possible to ascertain the identity and the location of the relevant parties. For the proprietary effects of transactions relating to cryptocurrencies within the system, the principle embodied in recital 38 of the Rome I Regulation – according to which the law that applies to the contract between the assignor and assignee under that Regulation "also applies to the property aspects of an assignment, as between assignor and assignee, in legal orders where such aspects are treated separately from the aspects under the law of obligations" might serve

135 In the opinion of Florence Guillame, "'*Blockchain* : le pont du droit internatonal privé entre l'espace numérique et l'espace physique," in Ilaria Pretelli (ed), *Conflict of Law in the Maze of Digital Platforms* (Schultess 2018), 180, in the absence of a valid choice of law agreement, the *lex fori* would be applicable, since any territorial connecting factor would be devoid of any relevance in DLT's settings.

as a basis for discussion, at least in case the recently advanced proposition to create a legal identifier of securities for PIL purpose, which would make visible the applicable law as determined under the relevant conflict-of-law rules, will be adopted and extended to crypto assets.[136]

All in all, the elective *situs* approach resonates both with the overall concept of DLTs, as a "space" where party autonomy, as embedded into the digital processes (*i.e.*, the code), creates the assets and handle them, and with the notional value of cryptocurrencies. Yet, the spontaneous process of aggregation underlying the establishment of DLT systems – at least the permissionless ones – calls for fall-back rules, based on objective connecting factors, that pursue predictability of the applicable law. Identifying the relevant party for whom, primarily, predictability should be achieved is only one of the manifold challenges ahead for lawmakers. Finding a compromise between the temptation to walk along well-known paths and the feeling (or fear) that new technologies discard even the need for (private international) law is, of course, a preliminary one.

136 Philipp Paech, "Conflict of Laws and Relational Rights," in Louise Gullifer and Jennifer Payne (eds), *Intermediation and Beyond* (Oxford: Hart 2019), 305–307.

PART 3

Specific Blockchain Assets & Legal Relations

CHAPTER 12

The Law(s) Applicable to Central Bank Digital Currencies

Caroline Kleiner

As of the date of writing of this contribution, Central Bank Digital Currencies (CBDCs) do not exist, or exist on an infinitely small scale. Indeed, according to the most recent BIS paper published on CBDC,[1] "To date, only two CBDCs have gone live (the Sand Dollar in The Bahamas and DCash in the Eastern Caribbean)." Most central banks are considering the introduction of CBDCs but have not decided yet whether they should issue them, and if so, under which policy scheme. Central banks are still either in the thinking process,[2] or in the experimental phase.[3] Even if some "foundational principals and core features of central bank digital currencies" have already been elaborated by the BIS jointly with seven major central banks,[4] the discussion as to whether, when and how this will happen is still ongoing.[5] Therefore, assessing the applicable law to a concept that is barely in existence is quite a challenge.

1 Raphael Auer et al., "CBDCs beyond borders: results from a survey of central banks: BIS Papers No 116" (*Bank for International Settlements* (*BIS*), June 2021), 6 <https://www.bis.org/publ/bppdf/bispap116.pdf> accessed 29 May 2022.

2 For instance, the ECB announced in July 2021 that it launched an investigation phase for the design of a potential digital euro until 2025. The BIS is also supportive of various initiatives of cooperation between central banks and created the "Innovation Hub work on central bank digital currency (CBDC)." The ECB, the Bank of England, the Federal Reserve, the Bank of Canada, the Bank of England, the Bank of Japan, the European Central Bank, the Sveriges Riksbank and the Swiss National Bank, together with the Bank for International Settlements (BIS), have created a group to share experiences as they assess the potential cases for central bank digital currency (CBDC) in their home jurisdictions. The group will closely coordinate with the relevant institutions and forums - in particular, the Financial Stability Board and the Committee on Payments and Market Infrastructures (CPMI).

3 China's CBDC is already in trial with some 24 million users and should launch the digital yuan in 2022.

4 The Bank of Canada et al., "Central bank digital currencies: foundational principles and core features" (*BIS*, 9 October 2020) <https://www.bis.org/publ/othp33.htm>.

5 Not to mention the interrogation on the legal basis for the issuance of CBDC, which might be controversial or need the modification of monetary laws: Phobeus L. Athanassiou, "Wholesale central bank digital currencies: an overview of recent central bank initiatives and lessons learned," in *ESCB Legal Conference 2020* (Frankfurt am Main: European Central Bank 2021),

© CAROLINE KLEINER, 2023 | DOI:10.1163/9789004514850_014
This is an open access chapter distributed under the terms of the CC BY-NC-ND 4.0 license.

The challenge is greater when one realises the breadth of the technological and operational range that can be used to implement CBDC. And each technological and operational choice is likely to entail different legal relationships (property rights or rights of claim), as well as direct or indirect relationships between the final user and the central bank. As such, it seems necessary to alert the reader of the prospective nature of this contribution, which asks more questions than it can answer. More than twenty years ago, international payments were qualified, in terms of conflict of laws, as quite "intractable."[6] If this was true when digital currencies had not yet come into existence or even been conceptualised, we wonder which adjective should be used to describe the legal difficulties encountered today....

If CBDCs – as one can assume – are likely to become a reality within the next few years, they may be created based on Distributed Ledger Technology (DLT), *i.e.*, using blockchain technology.[7] For instance, recent experiments of wholesale CBDC made by the *Banque de France* with the private sector, involved the simulation of a private blockchain issuing and settling unlisted and listed securities. In other words, settlements were simulated by CBDC issued on the blockchain.[8] However, the Report on a Digital euro envisages the use of various technologies, notably but not necessarily DLT.[9] Other research on the issuance of CBDCs does not necessarily advise the use of DLT; quite the contrary![10]

---

202 and Papapaschalis, "Retail central bank digital currency: a (legal) novelty?," in *ESCB Legal Conference 2020* (Frankfurt am Main: European Central Bank 2021), 214.

6 Luca Radicati di Brozolo, "International Payments and Conflicts of Laws" (2000) 48 American Journal of Comparative Law 307, 326.

7 The blockchain being one type of DLT: Dominique Legeais, *Blockchain et actifs numériques* (2nd edn, Paris: LexisNexis 2021), 19.

8 Valérie Fasquelle,"CBDC: how central banks approach innovation," in *ESCB Legal Conference 2020* (Frankfurt am Main: European Central Bank 2021), 189; Legeais (n 7), 165.

9 European Central Bank (ECB), "Report on a digital euro" (*ECB*, October 2020), 40 <https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf> accessed 29 May 2022.

10 David Chaum, Christian Grothoff, and Thomas Moser, "How to issue a central bank digital currency: SNB Working Papers" (*Schweizerische Nationalbank* (*SNB*), March 2021), 3 <https://www.snb.ch/n/mmr/reference/working_paper_2021_03/source/working_paper_2021_03.n.pdf> accessed 29 May 2022. The authors recommend the use of "a token-based, software-only CBDC without DLT." They argue that "DLT is an interesting design if no central party is available or if the interacting entities are not willing to agree on a trusted central party. However, this is hardly the case for a retail CBDC issued by a *central* bank. Distributing the central bank's ledger with a blockchain merely increases transaction costs; it does not provide tangible benefits in a central bank deployment. Utilizing DLT to issue digital cash may be useful if there is no central bank to start with (...) or if the explicit intention is to do without a central bank (*e.g.* Bitcoin)."

According to economists, "[w]hile most of the ongoing experiments are based on DLT, it is unclear whether the same technology would be used for full-scale implementations."[11] Either way, the possible use of this technology justifies the inclusion of this topic within the framework of this book.

The uncertainty regarding the technology adopted by central banks to issue their digital currency raises nonetheless a crucial question related to our topic: should the determination of the law or the laws applicable to CBDC be different according to the kind of technology used, *i.e.*, whether or not DLT is used? On the one hand, it is undeniable that technology has a powerful impact on the analysis of conflicts of laws. One only has to look at the evolution of conflict-of-laws rules related to contracts, and more specifically to consumer contracts, with the development of e-commerce.[12] And as this book shows, one should expect specific conflict-of-laws rules for smart contracts, *i.e.*, contracts concluded via blockchain.[13] On the other hand, the kind of technology used for the issuance of retail CBDC will presumably not be known by retail users. Hence, introducing a distinction for the determination of the applicable law, according to the technology used, could bring legal uncertainty. Since each CBDC might use different technologies, this legal risk should be avoided especially when establishing a new form of payment. Finally, the interoperability of the various issued CBDCs call for a homogenous conflict-of-laws rule, regardless of the specific technology used. For these reasons, the analyses of the conflict of laws put forward in this contribution should be technology neutral, *i.e.*, conducted regardless of the technology used, be it DLT or a centrally controlled infrastructure.[14]

---

11 Auer et al. (n 1), 13.

12 Article 6 of the Rome I Regulation (Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), [2008] OJ L177/6) on the law applicable to consumer contracts focuses on the "direction" of the activities, rather than Article 5 of the 1980 Rome Convention (1980 Rome Convention on the law applicable to contractual obligations (consolidated version), [1998] OJ C027), which referred to the "specific invitation to conclude the contract," "reception of the order," and "place where the order is given," traditional connecting factors that were not suited for e- commerce.

13 See Chapter 17 of this book by Mehdi El Harrak, "Do Smart Contracts Need New Conflict-of-Laws Rules?".

14 The better description of the differences between DLT and "conventional" infrastructures is the one authored by Raphael Auer and Rainer Böhme, "The Technology of Retail Central Bank Digital Currency" (*BIS Quarterly Review*, 1 March 2020), 92 <https://www.bis.org/publ/qtrpdf/r_qt2003j.htm>, and this description is worth citing here: "[c]onventional and DLT-based infrastructures often store data multiple times and in physically separate locations. The main difference between them lies in how data are updated. In conventional databases, resilience is typically achieved by storing data over multiple physical nodes, which are controlled by one authoritative entity, the top node of

The scope of the contribution will focus only on the cross-border use of CBDC, a situation prone to create conflicts of laws. The cross-border use is understood here as a situation of cross-border payment, that is, payment where the payer/debtor and the payee/beneficiary are located in different countries, and when the payment implies the use of a currency that is not common to both parties (one party pays or receives a payment in a currency which is not the one in force in the State where he/she is domiciled) (cross-currency payment). Even though international payments do not necessarily imply a cross-currency operation,[15] as it is the case for payments made within a monetary union composed of different states, the focus of this contribution should be the "extraterritorial use" of CBDCs.[16]

The determination of the applicable laws to a currency is not an easy matter in itself[17] and is subject to much theoretical legal debate. Determining the law or laws applicable to a CBDC seems even more difficult because of the impact of the technology used. The idea of this contribution is thus to ascertain whether proven solutions for "non-digital" or "conventional" currencies are still valid when it comes to CBDCs. This contribution will start by exploring what are CBDCs and what kind of legal relationship they could create (section 1). Then it will briefly recall the main principles of international law and conflict-of-laws rules used for "conventional" currencies (section 2), before assessing whether those solutions can still be used for the future CBDCs, in other words, whether new wine can be filled into old bottles (section 3).

---

a hierarchy. By contrast, in many DLT-based systems, the ledger is jointly managed by different entities in a decentralised manner and without such a top node. Consequently, each update of the ledger has to be harmonised between the nodes of all entities (often using algorithms known as 'consensus mechanisms'). This typically involves broadcasting and awaiting replies on multiple messages before a transaction can be added to the ledger with finality."

15 See BIS et al., "Central bank digital currencies for cross-border payments: Report to the G20" (*BIS*, July 2021), 3 <https://www.bis.org/publ/othp38.pdf> accessed 29 May 2022.

16 The experiment conducted by various central banks already tackles the issue of their international use and thus how their schemes should be coordinated: Project mCBDC Bridge is testing inter-operability between CBDC systems of four different jurisdictions (The Hong Kong Monetary Authority, the Bank of Thailand, the Digital Currency Institute of the People's Bank of China and the Central Bank of the United Arab Emirates) on the same DLT platform, while Project Dunbar is exploring the inter-operability between multiple CBDCs on a shared platform (Reserve Bank of Australia, Bank Negara Malaysia, Monetary Authority of Singapore, and South African Reserve Bank).

17 For money is a paradoxical, ubiquitous, and phantomatic concept: Caroline Kleiner, "Money in Private International Law: What Are the Problems? What Are the Solutions?" (2009) 11 Yearbook of Private International Law, 566.

1 What are CBDCs?

1.1 *Definition and the Different Options*

CBDCs may be created according to different schemes that will briefly be described. The 2021 BIS annual report defines CBDCs as "a form of digital money, denominated in the national unit of account, which is a direct *liability* of the central bank.[18] CBDCs can be designed for use either among financial intermediaries only (*i.e.* wholesale CBDCs), or by the wider economy (*i.e.* retail CBDCs)."[19] Put more simply, CBDCs are seen as a digital form of central bank money in use today: cash (*i.e.* coins and banknotes) and central bank settlement accounts. CBDCs are electronic central bank liabilities that can be used in peer-to-peer exchanges and are universally accessible.[20]

As these definitions suggest, a distinction should be made between wholesale CBDCs (or interbank use of CBDCs) and retail CBDCs. One could, however, consider that wholesale CBDCs already exist,[21] since the relationship between commercial banks on the one side and between commercial banks and central banks on the other side already use digital currencies. Hence, the true question to be addressed in this chapter relates to the issuance of CBDCs for all citizens, *i.e.*, retail CBDCs. This contribution will thus focus on the applicable laws to CBDCs used for retail cross-border payments.

Another crucial distinction to be made concerns the scheme decided by the central banks for the issuance of CBDCs. Two modalities are currently discussed. Either CBDCs will be issued as a right of claim (hypothesis of "account-based") or as a right of ownership (hypothesis of a "token based" or "bearer instrument"). The first option, the "account-based system" follows the conventional account model and ties the right to use CBDCs to a *person* with a known identity. The second one requires the CBDC user to demonstrate knowledge of an encrypted value.[22] It offers universal access and protects privacy.

18 This will not be discussed in this contribution, for it would go beyond our subject; the issue as to whether the currency issued by a central bank shall be analysed as a *liability*. For this debate, see Michael Kumhof et al., "Central Bank Money: Liabiliy, Asset, or Equity of the Nation?" (*Rebuilding Macroeconomics*, 25 November 2020) <https://www.rebuildingmacroeconomics.ac.uk/publications>.

19 BIS, "BIS Annual Economic Report 2020/21" (*BIS*, 29 June 2021), 65 <https://www.bis.org/about/areport/areport2021.pdf>.

20 Morten Linnemann Bech and Rodney Garratt, "Central bank cryptocurrencies" (*BIS Quarterly Review*, 17 September 2017), 57 <https://www.bis.org/publ/qtrpdf/r_qt1709f.htm>.

21 Chaum, Grotthof, and Moser (n 10), 2.

22 A private key would protect the private ownership of the holder of the wallet, whereas a public key would guarantee the security of the system, *i.e.*, the impossibility to duplicate

The choice of one or the other option could have a decisive impact on the applicable law.

Either way, central banks may decide to operate directly or indirectly. The issuance of CBDCs in direct or "1-tier form"[23] would give direct access, by the final users, to either an account opened and managed by the central bank itself, or a "digital wallet" containing CBDCs as tokens directly distributed by the central bank. If the issuance is indirect or under a "2-tier form," CBDC accounts or CBDC digital wallets would be administered by intermediaries licensed to distribute CBDCs. This option will also have an impact on the applicable law, since the participation of intermediaries in the operation gives rise to the applicability of the law governing the intermediary's activity.

1.2 *The Reasons to Create CBDCs*

Different factors explain the converging idea of many central banks to create CBDCs.[24] Many states, central banks, and other monetary institutions, as well as international organisations focusing on the international monetary and financial system[25] expressed concerns over the rapid expansion of private and self-called "cryptocurrencies."[26] States struggle on their qualification and

---

it. Both keys would be calculated and delivered by the central bank which guarantees the reality/veracity of the CBDC token.

23 To use the expression of Wouter Bossu et al., "Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations: IMF Working Paper WP/20/254" (*International Monetary Fund*, 20 November 2020), 10 <https://www.imf.org/en/Publications/WP/Issues/2020/11/20/Legal-Aspects-of-Central-Bank-Digital-Currency-Central-Bank-and-Monetary-Law-Considerations-49827>.

24 The ECB mentions no less than seven reasons to issue CBDC: "A digital euro could be issued (i) to support the digitalisation of the European economy and the strategic independence of the European Union; (ii) in response to a significant decline in the role of cash as a means of payment, (iii) if there is significant potential for foreign CBDCs or private digital payments to become widely used in the euro area, (iv) as a new monetary policy transmission channel, (v) to mitigate risks to the normal provision of payment services, (vi) to foster the international role of the euro, and (vii) to support improvements in the overall costs and ecological footprint of the monetary and payment systems." ECB (n 9), 9.

25 See for instance the concerns expressed by the Financial Action Task Force (FATF) in the updated guidance for a risk-based approach: FATF, "Virtual Assets and Virtual Asset Service Providers" (*FATF*, October 2021) <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf> accessed 29 May 2022.

26 Although it is interesting to note that according to the BIS Annual Economic Report 2020/21 (n 19), "by now, it is clear that cryptocurrencies are speculative assets rather than money, and in many cases are used to facilitate money laundering, ransomware attacks and other financial crimes. Bitcoin in particular has few redeeming public interest attributes when also considering its wasteful energy footprint," 67. See also Benjamin C. Cohen,

are hesitant on the regulation they should enforce.[27] In our view, it cannot be monetary law, as "cryptocurrencies" developed privately on different types of blockchain[28] do not satisfy the definition of money.[29] The fear exists that those new objects might compete with the existing national monetary units, which in turn might lead to a disorganisation of the international monetary system with significant risks for international financial stability.[30]

A second factor lies in the rise of stablecoins, *i.e.* crypto assets whose value is pegged to one or a basket of national currencies or even gold. The *Diem* project launched by Facebook (formerly under the name *Libra*) has been a "wake-up call" for financial supervisors and monetary authorities, even though it has been dropped out.[31] The competition with national currencies (and the

---

"The Bonfire of cryptocurrencies?" (*Project Syndicate*, 29 October 2021) <https://www.project-syndicate.org/onpoint/cash-cryptocurrencies-future-of-money-by-benjamin-j-cohen-2021-10> "according to the International Monetary Fund, there are around 9,000 digital tokens listed on various exchanges today. Earlier this year, the market value of all crypto assets surpassed $2 trillion – a tenfold increase in not much more than a year."

27 In the US, various public agencies are concerned with cryptocurrencies (SEC, CFTC, IRS, OCC) and each one could apply their regulation. In the EU, see Chiara Zilioli, "Crypto-Assets: Legal Characterization and Challenges under Private Law" (2020) 46 European Law Review 251, 252, who emphasises that it is unclear whether cryptocurrencies fall within the scope of the Electronic Money Directive (EMD2), the Payment Services Directive (PSD2) or the Markets in Financial Instruments Directive (MiFID2). The difficulty is about to be overcome with the Proposal for a regulation of the European parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 COM(2020)/593 final. It is noteworthy that this Regulation, when adopted, will not apply to "the European Central Bank, national central banks of the Member States when acting in their capacity as monetary authority or other public authorities" (Article 3(a)). Hence, CBDC will not be in the scope of this Regulation. On the variety of legal regimes applicable to crypto assets and the call for a global regime, see Matthias Lehmann, "National Blockchain Laws as a Threat to Capital Markets Integration" (2021) European Banking Institute Working Paper Series 2021 No 95.

28 Legeais (n 7), 18.

29 Caroline Kleiner, "Cryptocurrencies as transnational currencies?," in Christoph Benicke and Stefan Huber (eds), *Liber amicorum Herbert Kronke, National, International, Transnational: Harmonischer Dreiklang im Recht - Festschrift für Herbert Kronke zum 70. Geburtstag am. 24 Juli 2020* (Bielefeld: Ernest and Verner Gieseking 2020), 985. The fact that El Salvador has decided to "make Bitcoin legal tender" (sic) does not change our analysis. The "Bitcoin" still refers to the US dollar as a unit of account. See our comment on this Act: Caroline Kleiner, "Chronique de droit bancaire international" (2021) 1 Revue de droit bancaire et financier 15, 16.

30 Hossein Nabilou, "Testing the waters of the Rubicon: the European Central Bank and central bank digital currencies" (2020) 21 Journal of Banking Regulation 299.

31 Dirk A. Zetzsche, Ross P. Buckley, and Douglas W. Arner, "Regulating Libra: The Transformative Potential of Facebook's Cryptocurrency and Possible Regulatory Responses" (2019) European Banking Institute Working Paper Series 2019 No 44, 4; see also Hubert

superpower that would have acquired Facebook by releasing this unit) seemed more severe than the threat from the private cryptocurrencies. Because stablecoins seem to offer a more stable value, they could more easily replace the national currencies in payment and as units of account.[32] The emergence of these new products has therefore only increased the need for central banks to adjust their offer to new forms of transactions and payment.

Other incentives also come into play. For its development, international trade needs efficient cross-border payment systems. The G20 set itself the task to promote the efficiency of cross-border payments involving a cross-currency transaction.[33] This objective is very clearly stated in all published reports and speeches made by the heads of monetary institutions.

Another objective is more concerned with the social benefit derived from the creation of CBDCs. Certain authors mention that the development of CBDCs could foster financial inclusion,[34] an observation concurred with central banks financial programs related to the COVID-19 government to support the economy, such as loans or financial assistance, which could have been distributed more quickly if they had been directly transferred to accounts in CBDCs (upon the condition that the central banks would have a direct access to such accounts).[35]

Finally, the issuance of CBDCs could also serve the purpose of a better and more efficient transmission of monetary policies. In a common article, Zellweger-Gutknecht, Geva and Grünewald argue that in light of the decline of cash, the issuance by the European Central Bank (ECB) of CBDCs would help the ECB and the European System of Central Banks (ESCB) to fulfil their primary objectives: price stability and the smooth operation of payment systems. A digital euro would improve the supply of information to the central bank and would become a medium of monetary policy, even though, according to

---

de Vauplane, "Les défis juridiques du Libra et plus généralement des cryptomonnaies" (2020) 1 Revue de droit bancaire et financier 1, 2.

32 At least, this is the claim of the creators of many stablecoins. States fear that replacement: see G7 Working Group, "G7 Working Group on Stablecoins: Investigating the impact of global stablecoins" (*BIS*, October 2019) <https://www.bis.org/cpmi/publ/d187.pdf> accessed 29 May 2022.

33 Auer (n 1), 3.

34 ECB (n 9), 3, 9, 10, 12, 15, 20; see also Corinne Zellweger-Gutknecht, Benjamin Geva and Seraina Neva Grünewald, "Digital Euro, Monetary Objects, and Price Stability: A Legal Analysis" (2021) 7 Journal of Financial Regulation 284, 305.

35 See Lael Brainard, "Private Money and Central Bank Money as Payments Go Digital: an Update on CBDCs" (*Federal Reserve*, 24 May 2021), 3 <https://www.federalreserve.gov/newsevents/speech/brainard20210524a.htm>.

those authors, the use of the digital euro as a new policy transmission method is not legally permitted for the time being.[36]

1.3 *The Impact on Monetary Sovereignty of the Issuance and International Use of CBDCs*

A reflection on the international use of CBDCs and the legal consequences it might have also requires consideration of the impact of CBDCs on the core concept in international law, that is, monetary sovereignty. According to the 2021 BIS annual report, "CBDC design can protect monetary sovereignty by making legitimate cross-border and cross-currency payments easier, thereby obviating the need to hold other currencies and helping a central bank to monitor transactions."[37] The issuance of CBDCs might then protect the national monetary unit and therefore monetary sovereignty, in the sense that the monopoly of the national monetary unit will not be endangered by other competitors. In that regard, issuance by central banks of CBDCs is a manifest reaffirmation of monetary sovereignty, which justifies the application of the *lex monetae*. Before seeing how these new forms of central bank money can be disruptive from a PIL perspective, we will briefly deal with the question of the law applicable to money, and more particularly the law applicable to international payments.

2 What Are the Laws Applicable to Money?

Determining the laws applicable to a currency requires an analysis of the nature of money from a legal point-of-view, and more specifically, from a Private International Law (PIL) perspective.[38] The classic distinction made in economics is between means of payment, of storage and unit of account. However, from a legal perspective, another categorisation is permitted, and needed. Along with other legal scholars,[39] we have explained that money consists in the link that exists between two kinds of *units* that each serves a specific function: a function of evaluation (through the unit of account) and a function of payment (through the unit of payment). Both functions nowadays, share the same name (*i.e.*, the euro, the dollar, the franc…), though their nature, as well as their

36 Zellweger-Gutknecht, Geva, and Grünewald (n 34), 312.

37 BIS (n 19), 10

38 Kleiner (n 17), 569.

39 Rémy Libchaber, *Recherches sur la monnaie en droit privé*, preface by Pierre Mayer (Paris: LGDJ 1992), 20 and Karl Olivecronna, *The Problem of the monetary Unit*, (Stockholm: Almqvist & Wiksell 1957), 135.

regime, is quite different. If a "thing" assumes one function without the other, that "thing" does not qualify as "money". Both functions relate to two inseparable but distinct aspects of money: the abstract and the concrete.[40] Each of these facets of money involves the application of a specific body of rules.[41]

2.1 *The Law Applicable to the Abstract Aspect of Money*

Each state uses a monetary unit to serve as a unit of value for its economy. The enactment of a monetary unit is the heart of an economy. Abstract money, as a unit of account, is governed by the law of the state that declared that monetary unit *as its own*, *i.e.* the law of the state that gave it a name and a value reference system. This rule is also coined as the *lex monetae.* This rule enshrines a principle of international law,[42] recognised by the Permanent Court of International Justice,[43] notwithstanding the formula of the "conflict-of-laws rule" that some instruments, such as Article 147(1) of the Swiss Private International Law Act, still use.[44]

The scope of the *lex monetae* covers the name of the currency as well as its value, more precisely the method according to which the value is calculated.[45] But limiting the scope of the *lex m*onetae only to these two elements would correspond to a narrow interpretation. Since the concept refers to a currency – as a specific unit of account in force in a State – the scope of the *lex monetae* should also extend to the monetary policy rules, and as has shown the introduction of the euro more than twenty years ago, to the principle of continuity of legal instruments.[46] Monetary policy is a concept that has also evolved,

40 Libchaber (n 39); Olivecrona (n 39), 119.

41 The following analyses rely on our previous work: Caroline Kleiner, *La monnaie dans les relations privées internationales,* preface by Pierre Mayer (Paris: LGDJ 2010), 93.

42 Charles Proctor, *Mann on the Legal Aspects of Money* (7th edn, Oxford: Oxford University Press 2012), 367. See *contra* Michael Gruson, "The Scope of Lex Monetae in International Transactions: a United States Perspective," in Mario Giovanoli (ed), *International Monetary Law: Issues for the New Millennium* (Oxford: Oxford University Press 2000), 433–456, No 23.02.

43 Permanent Court of International Justice (P.C.I.J.), *Case concerning the Payment of Various Serbian Loans Issued in France: France v. Kingdom of the Serbs, Croats and Slovenes*, 1929 P.C.I.J. (ser. A) No. 20 (July 12), 44.

44 The same analysis holds for Art. 2.646(1) of the Romanian Civil Code. On the Swiss PILA, see Kleiner (n 17), 578.

45 See among others: Bertold Wahlig, "European Monetary Law: The Transition to the Euro and the Scope of the Lex Monetae," in Mario Giovanoli (ed), *International Monetary Law: Issues for the New Millennium* (Oxford: Oxford University Press 2000), 121–136, No 6.06.

46 See Jean-Victor Louis, "The New Monetary Law of the European Union," in Mario Giovanoli (ed), *International Monetary Law: Issues for the New Millennium* (Oxford: Oxford University Press 2000), 137–159, No 7.37

along with the evolution of the concept of money. *Stricto sensu,* monetary policy covers matters related to the management of the monetary unit only. *Largo sensu*, monetary policy concerns also issues related to the payment system,[47] which is one of the bases of the guarantee of financial stability, a common objective to many central banks.

2.2 *The Law Applicable to the Concrete Aspect of Money*

What we call "concrete money" corresponds in this contribution to money when it is *used* to transfer a certain amount of purchasing power. Today, two fundamental forms of money in circulation coexist: banknotes and coins, issued by the monetary authority, which, accordingly, are a *direct liability* of central banks, which explains why this form of money is qualified as "central bank money;" and book money, which is managed by "commercial banks" through the accounts constituted by the deposits received and the credits granted by commercial banks.[48] Book money is exchanged *au-par* with central bank money. This distinction is well known by jurists, but not necessarily by currency users. Those two types of currency, whatever their form, look the same*;* yet the set of rules applicable to their circulation differ. Consequently, no uniform conflict-of-laws rule related to international payment exists.

Payment, being the performance of an obligation, is governed by the law applicable to the obligation, the *lex causae*.[49] However, it has already been shown that other laws may also come into play to govern the particular payment transaction, which involves, depending on the method of payment chosen, a contractual relationship other than that between the payer and the payee. Indeed, in any payment transaction, there is always an additional party at the table of the parties to the original relationship, and this additional presence implies the application of a third law in addition to the *lex causae*. We will briefly address those *additional* applicable laws.

2.2.1 When the Payment Is Made with Cash or "Central Bank Money" (Payment 1.0)

As of today, and even if this means of payment is in constant decline, monetary payment may still be made through a delivery of cash: banknotes and coins which have legal tender. For the purpose of this contribution, this form

47 Francesco Martucci, *L'ordre économique et monétaire de l'Union européenne*, preface by Doninique Carreau (Brussels: Bruylant 2016), 105.

48 The word "commercial bank" here is used widely and targets all kind of financial institutions receiving deposits and granting loans.

49 Radicati di Brozolo (n 6), 318; Proctor (n 42), 113.

of payment can be labelled Payment 1.0. Determining the law applicable to the transfer of rights of a holder of a coin or banknote can go in two directions.

The first one is to look at the coins or banknotes as chattels and apply to them the *lex rei sitae*. But this conception is obsolete.[50] The second and preferred option consists in seeing in those objects not their material nature, but the fact that they exist because of the legal tender. Legal tender means that the payee must accept the coins or banknotes delivered for their face value.[51] It serves the purpose of guaranteeing the payer that, by delivering to the payee the quantity of monetary units stipulated on the coin or the banknote, its debt will be extinguished, because a banknote of 50 euros, for instance, must be received for the value equivalent of 50 euros, no less and no more, whatever is the intrinsic value of the paper.

Legal tender does not mean that cash shall always be accepted in a monetary payment transaction.[52] Indeed, many states, mostly for fiscal reasons, prevent the payment of high amounts of cash, or of certain operations in cash, for practical reasons.[53] Legal tender is enacted by the law of the issuing state (or union of states) of the material monetary representations. In the case of the euro for example, legal tender of euro banknotes and coins has been enacted by Regulation 974/98 of 3 May 1998 on the introduction of the Euro[54] and Regulation 2866/98 of 31 December 1998[55] on the conversion rates between the Euro and the currencies of the Member States adopting the Euro. The international cash payment is thus *per se* governed by the law of the issuing authority.

2.2.2 When the Payment Is Made through Book Money or "Private Money" (Payment 2.0)

Payment today might also be performed through the transfer of monetary units deposited in a bank or payment account of the payor to the account of the beneficiary. The most salient aspect of this form of payment, from a PIL perspective, is the presence of at least one intermediary to perform the payment. Consequently, the applicable law to the contractual relationships

50 Proctor (n 42), 31; Kleiner (n 41), 139.

51 See Proctor (n 42), 74.

52 See in EU law: ECJ, *Johannes Dietrich and Norbert Häring v Hessischer Rundfunk*, Joined Cases C-422/19 and C-423/19.

53 See for example Article L. 112-6 of the French Monetary and Financial Code.

54 Council Regulation (EC) No 974/98 of 3 May 1998 on the introduction of the euro, [1998] OJ L139, 1–5.

55 Council Regulation (EC) No 2866/98 of 31 December 1998 on the conversion rates between the euro and the currencies of the Member States adopting the euro, [1998] OJ L359, 1–2.

between the intermediary and its client, denominated in French, *la loi de la banque,* comes into play.

The law governing the contractual relationship with the bank can be the law chosen by the parties,[56] with all the caveats provided for by consumer law. Absent a choice of law, the law of the state where the payor's bank is located can also be applied as it is the place where the service provider has its habitual residence[57] or where the operations of payment are being performed (or technically supervised). It does not matter whether the bank is a branch of a bank established abroad or has its registered office in the same state: the law of the place where the payor's bank manages the account is applicable.[58] This solution favours legal certainty, insofar as many rules relating to bank accounts are mandatory rules (*lois de police*). The UNCITRAL Model Law on International Credit Transfers,[59] which concerns only substantial rules relating to international payments, proposes however, in a footnote, a conflict-of-laws rule. This rule provides that "the rights and obligations arising out of a payment order shall be governed by the law chosen by the parties. In the absence of agreement, the law of the state of the receiving bank shall apply."[60] But this proposal has not met with great success, to say the least.

With respect to scope, the law governing the contractual relationships between the holder of a bank account and the bank will decide various issues, such as the date and the place of the payment, which can be either in the state of the payor or in the state of the beneficiary. Whatever the law applicable to the means of payment, this law needs to be coordinated with the law of the place of performance.

2.3 *The Law of the Place of Performance* (*lex loci solutionis*)

The *lex loci solutionis* was forged at a time when payment was made in person, by the delivery of a chattel in payment. Even if the means of payment have tremendously evolved, the rule is still in force today in many instruments. For

56 In accordance with Article 3 of the Rome I Regulation (n 12); Article 116 of the Swiss Private International Law Act (Federal Act on Private International Law (PILA) of 18 December 1987, RS 291), and the general principle of party autonomy.

57 Article 4(1)(b) of the Rome I Regulation (n 12); Article 117 of the Swiss Private International Law Act.

58 Kleiner (n 41), 145.

59 Adopted by UNCITRAL on 15 May 1992. UNCITRAL, *UNCITRAL Model Law on International Credit Transfers* (New York: United Nations Publications 1994). The full text is available at: <https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/ml-credittrans.pdf>.

60 Radicati di Brozolo (n 6), 317.

instance, even if Article 12(1) of the Rome I Regulation provides that the law applicable to a contract governs its performance, the second paragraph of the provision states that: "[i]n relation to the manner of performance and the steps to be taken in the event of defective performance, regard shall be had to the law of the country in which performance takes place."[61]

An interesting and specific aspect of the use of cash for payment is that it is materialised, in the sense that it necessarily occurs in a specific state. In that case, the *lex loci solutionis* can easily be identified. Thus, if the law of the state where the payment shall take place contains a rule prohibiting the payment with cash beyond a certain amount, this law should be taken into consideration. As the recent ECJ *Hessischer Rundfunk* case[62] showed, a distinction should be made between the power to declare legal tender, which lies in the exclusive competence of the EU, in the area of monetary policy for the Member States whose currency is the euro, and the exercise by a Member State of its own competence to exclude the possibility of discharging an obligation in banknotes denominated in euro, "provided (i) that legislation does not have the object or effect of establishing legal rules governing the status of legal tender of such banknotes; (ii) that it does not lead, in law or in fact, to abolition of those banknotes, in particular by calling into question the possibility, as a general rule, of discharging a payment obligation in cash; (iii) that it has been adopted for reasons of public interest; (iv) that the limitation on payments in cash which the legislation entails is appropriate for attaining the public interest objective pursued; and (v) that it does not go beyond what is necessary in order to achieve that objective, in that other lawful means of discharging the payment obligation are available."[63] In other words, it is considered – at least in EU law – that the scope of the *lex monatae* does not go as far as the acceptability of a particular form of payment.[64] The acceptability of a certain means of payment remains under the control of the law of the state of the place of performance.

When payment is made through a transfer, the concept of the "place of the payment" becomes more artificial, in the sense that the localisation can be

61 A more detailed analysis of the *lex loci solutionis* may be found in Kleiner (n 41), 294.

62 *Hessischer Rundfunk* (n 52).

63 *Id.*, para. 78.

64 For a criticism of this interpretation: Helmut Siekmann, "Restricting the Use of Cash in the European Monetary Union" (2016) Institute for Monetary and Financial Stability Working Paper Series No. 108, 20. In the same vein: see the US Supreme Court, according to which "[e]very contract for the payment of money simply is necessarily subject to the constitutional power of the government over the currency, whatever that power may be, and the obligation of the parties is therefore assumed with reference to that power," *Legal Tender Cases*, 79 U.S. 457, 549 (1870).

made only on a legal basis, not on a factual basis. Indeed, the legal localisation of a payment depends on the legal conception of payment, which can be influenced by civil law rules on the determination of the place of payment[65] and by the analysis of commercial (or banking) law rules, which determine exactly when the final payment is made, depending on the instrument used.[66] The difficulty to determine the place of payment is increased with the use of a currency which is not the currency of the state where the payment service provider is located, and which requires the participation of a corresponding bank, established in the state of the currency used for the payment.[67] For this form of *delocalised* payment, the *lex loci solutionis* is of a declining importance. Yet some conflict-of-laws rules continue to insert the determination of the currency of payment in the scope of the law of the place of payment.[68]

3 Are New Rules of PIL Needed When CBDCs Will Be Issued?

It is striking to note that the international use of CBDCs is not always taken into consideration by various research studies and that when it is, the issues of PIL are not at all addressed. As if the fact that the technology is without borders, so are the legal monetary relationships which use that technology.[69] This absence could also be justified by the idea that "Code is law,"[70] in the sense that the code enshrines itself rules of law.[71] States however remain and so do their

65 For instance: Article 1343-4 of the French Civil Code; §270 of the German Civil Code (BGB); Article 74 of the Swiss Code of Obligations.

66 In French law, according to Article L. 133-6 of the Monetary and Financial Code, which transposed Article 80 of the Directive (EU) 2015/2366 of the European parliament and of the council of 25 November 2015 on payment services in the internal market, [2015] OJ L337/35, 35–127, the date of the payment is deemed to be the date of reception of the funds by the beneficiary or by the payment services provider of the beneficiary. By contrast, the date of the payment made by check is the date when the bank of the drawer transfers the funds to the bank of the beneficiary.

67 Argument used by some states to justify the competence of their public authorities; hence their national legislation. See Kleiner (n 41), 306; Samuel L. Hatcher, "Circuit Board Jurisdiction: Electronic Payments and the Presumption against Extraterritoriality" (2020) 48 Georgia Journal of International and Comparative Law 591, 602.

68 See, for instance, Article 147(3) of the Swiss PILA, which sets forth: "The law of the state in which payment must be made determines in which currency such payment must be made" and Article 2.646(3) of the Romanian Civil Code.

69 See also Lehmann (n 27), 2.

70 Title of the famous article by Lawrence Lessig, "Code is Law: On Liberty in Cyberspace" (*Harvard Magazine*, 1 January 2000) <https://www.harvardmagazine.com/2000/01/code-is-law-html>.

71 Legeais (n 7), 51.

borders. The use of CBDCs will necessarily trigger conflict-of-laws situations.[72] The question to be answered is whether the introduction of this new *form* of money will disrupt existing solutions.

3.1 *New Legal Aspects and Risks*

One of the main incentives for central banks to issue CBDCs is to foster the efficiency of international payments.[73] Yet, the legal framework for the use of CBDCs in *international* payments has not attracted much attention.[74] The focus at the moment is almost exclusively on the technology and the different possible models for the implementation of CBDC payment systems. One issue is already taken for granted: the use of CBDCs will need another payment infrastructure. Indeed, current payment systems cannot be for CBDC international use: new routes are needed. Those routes may be different, according to the architecture selected by central banks. As explained by Auer, Haene and Holden, two different arrangements for the international use of CBDCs may be envisaged.[75]

The matrix of the first architecture would be interoperability between CBDC systems. This would require (if we understand correctly the different scenarios of "multi-CBDC arrangements") the conclusion of either bilateral agreements between central banks to make their CBDC system compatible, or multilateral agreements that would create a common clearing system (centralised or decentralised). Experiments conducted by various central banks currently test both types of arrangements.[76] Under this architecture, each CBDC would be governed by its own rule book (that is, the rules of the *lex monetae*). In our understanding, in this architecture, any cross-border payment with CBDC of country A made by a payor in country A to a beneficiary in country B would then require a conversion of CBDC A to CBDC B or currency B (if country B did not issue CBDC or if so wishes the beneficiary of the payment), as it is the case for book money payment. However, the difference could be that the exchange rate would already be "embedded" in the program, in the sense that

72 Mathias Audit, «Le droit international privé confronté à la blockchain» (2020) 4 Revue critique de droit international privé 669, 669.

73 See *supra*.

74 With the exception of Bossu et al. (n 23). The authors acknowledge the fact that CBDC raises new PIL issues but their research paper focuses on monetary law.

75 Raphael Auer, Philipp Haene, and Henry Holden, "Multi-CBDC arrangements and the future of cross-border payments: BIS Papers No 115" (*BIS*, 19 March 2021), 4 <https://www.bis.org/publ/bppdf/bispap115.pdf>.

76 See (n 16).

a link would be created to the formula according to which a specific rate of exchange is calculated.

The second scheme envisages the direct international use of CBDC, but such use can occur only if a central bank authorises non-residents to hold a CBDC of their own jurisdiction or authorise its use outside its territory. Again, those choices (and their feasibility) will themselves depend on the type of CBDC: either "account-based" or "token-based." The method of circulation of a CBDC and so the legal relationships deriving from a transaction made with CBDC will be different depending on those choices.

Allowing cross border payments with CBDC will also accrue the risk in the transaction. Whereas a payment with cash is simply performed by the delivery of the banknotes or coins, the payment with digital currencies implies electronic fingerprints or other methods of identification (*e.g.* FaceID), as it does already with electronic transfer of book money. This raises the risk of different levels of protection of personal data. The level of requirement in terms of application of KYC (Know Your Customer) and AML/FT (Anti Money Laundering/Financing Terrorism) might also be different among the CBDC jurisdictions.

3.2 *The Expanding Scope of the Lex Monetae or the Law of the Issuing Authority*

The issuance of CBDC will allow central banks to shape, in the software program designing CBDC, characteristics that so far escaped their capacity to control.[77] In this sense, CBDC can be viewed as "tailor-made" currency. Indeed, central banks will be able to decide (i) who may own CBDC; (ii) where it can be used and possibly (iii) at which rate it can be exchanged. But the two first choices seem to be possible only if the distribution of CBDC is made by following an account-based architecture.[78] First, contrary to monetary tokens issued until now by monetary authorities – coins and bank notes – central banks will actually have the power to control the circulation of the CBDC they will issue in terms of quality and quantity. Central banks may restrict the use of *their* CBDC to residents in their jurisdiction only, or on the contrary, extend the use to non-residents. Second, central banks would also be able to define the territory

77 Legeais (n 7), 9.

78 Indeed, the anonymity deriving from the very nature of a bearer instrument, on the contrary, should not permit central banks to select the criteria that a potential holder of CBDCs should meet, and the control of the extraterritorial circulation of the currency would then be – as far as we understand the technology – impossible, or at least more difficult.

where their CBDCs may be used,[79] *i.e.*, whether an "extraterritorial" use would be permitted. Third, we can also imagine that the program enshrines rules in order to determine the exchange rate, should the CBDC be convertible into other CBDCs or other national currencies.

Those characteristics depend on the policy decided by central banks. These choices will characterise the international character of CBDCs. In a way, those characteristics are close to the *convertibility* of a currency, which was known for a long time to be an aspect to be determined by the *lex monetae.*[80] However, attributing those characters will extend the scope of the *lex monetae,* which will be aligned with the new tools of the monetary policy, understood *lato sensu*.[81] In the same vein, application of a rate of interest (positive or negative) to the amount of CBDC in a digital wallet or in account, as well as the possibility to set a time limit for their use, show how far monetary policy measures will be directly embedded in the new currency.

However, the expansion of the *lex monetae* is not limited to those issues pertaining to monetary policy but goes beyond that sphere. Indeed, software program will also enable central banks to determine the kind of right final users will have over CBDCs (*e.g.* right of ownership or claim). In this context, is it worth enquiring as to the law applicable to the possession of CBDCs. Indeed, whether or not a CBDC account holder or the possessor of a "CBDC token" may claim its right of claim or ownership will depend on the law of the issuer which designed the characteristics of the CBDC. The second extension of the scope of the *lex monetae* concerns issues of privacy. The quantity of information that passes in the payment process will also be determined *electronically* upon the choices made by central banks. All those new characteristics, which exceed the domain of monetary law – even in its broadest sense –, will yet be governed by the law of the issuing central bank, *i.e.*, the *lex monetae.* This shows that the use of a specific currency always goes along with the application of the rules linked to this currency, as stated by the US Supreme Court in 1870.[82]

It is important here to note that the law applicable to the characteristics of CBDC should be the one of the central bank itself, and not the one of the issuing state. The distinction is relevant in the context of a "supranational" currency shared by a group of states, as is the case with the Euro Area. Applied to

79 If we accept the idea that a currency has a specific "territory," linked to the one of the State which enacted the currency as its legal currency.

80 Dominique Carreau and Caroline Kleiner, "Monnaie," in *Répertoire Dalloz de droit international* (Paris: Dalloz 2019), No 78.

81 See *supra.*

82 In the *Legal Tender Cases* (n 64), see footnote 64.

the Euro, the decision as to who may own a digital Euro and where it can be used lies in the competence of the ECB and the SECB and not in the competence of the Member States.[83] This is not a decision adopted by the legislative branch of government, but by the authority in charge of monetary policy. This tendency shows the growing importance of the role of central banks in the conduct of monetary policy *largo sensu* and that the *lex monetae* should probably be rephrased as the law *of the issuing central bank* (*or monetary authority*) and not the law of the issuing *country*. In the case of the Euro, no national law of a Eurozone member state shall apply to the digital euro; only the law as decided by the competent authorities in the Eurozone.

Given the manifest expansion of the scope of the *lex monetae*, there is no place for the application of any other law when CBDCs are used in an international payment.

3.3 *The Law Applicable to International Payments Made with CBDCs (Payment 3.0)*

As already mentioned, the law applicable to international payments is an ingenious combination of the *lex causae,* the law specific to the instrument used for the payment, and the *lex loci solutionis.* Is this combination still at stake with CBDC? In other words, may cross-border payment be regulated only with the application of the *law of the issuing authority,* which then will resolve all possible kinds of conflicts of laws by having already built, into the CBDC parameters, the mechanism that applies in case of conflict? Technology cannot be the answer, as all future events are not predictable and capable of being programmed. The following lists potential conflicts, and coordination needs are, for the same reason, not exhaustive.

3.3.1 The Determination of the Date of the Payment

The moment when the payment in CBDC is deemed to be final remains an issue not necessarily encompassed in the scope of *lex monetae.* So this issue might be left to *the lex causae.* Nonetheless, the application of the latter will be conditioned by the technicalities of the program designed by the law of the issuing authority. Coordination will then be needed.

83 The question whether the creation of a digital euro is feasible, from a legal point of view, without modifying the existing legal framework is not tackled in this contribution. For that question, see Zellweger-Gutknecht, Geva, and Grünewald (n 34); Bossu et al. (n 23).

3.3.2 The Determination of the Validity of the Payment

The main issue related to international payments in CBDC is probably whether a payment in CBDC is considered as such, in other words, whether the debtor has validly discharged his obligation to pay the creditor. If payor A in country A wishes to pay beneficiary B in country B with CBDC A, whereas country B does not allow payment in CBDC, (and assuming CBDC A can be held extra-territorially by a non-resident of country A), should the law of country B be "considered?" The situation resembles the one previously discussed involving cash, with the difference that the "place of payment" cannot be determined. Indeed, the concept of the *lex loci solutionis* disappears with the use of CBDC. The technology itself can be localised only with great difficulty and with legal fictions. But should this rule be replaced by another one, so that the law of the state which prohibits this kind of payment is at least considered? The application of the law of the state of the habitual residence of the beneficiary could be envisaged. However, if a payment can be final only if the law of the state of the habitual residence of the beneficiary says so, the application of this law would contradict the project – the program – of the law of the issuing authority. How should this conflict be resolved? By a balancing of interests approach?

Another interrogation relates to the coordination between the *law of the issuing authority* and a foreign freezing order. Let us imagine a payor located in country A who becomes the target of a freezing order issued by an authority of country B. According to the order, this person is prohibited to dispose of its assets, wherever they are located. However, the payment order of CBDC for a beneficiary located in country C has been given. Whether or not the payment is considered as valid will depend on the law applicable to the payment. How do we determine this law? Asserting that the law of country A, as the law of the issuing authority of CBDC A, will apply to the question, is far from satisfactory. It would not be possible to take into account the freezing order of country B. So the prohibition posited by country B should be considered as an overriding mandatory rule.

At present, we cannot imagine how a CBDC "program" could take into account all possible conflictual situations and hence the wide range of overriding mandatory rules that could come into play in the process of an international payment. Which law should be predominant, *i.e.*, the *lex monetae* or the overriding mandatory rule of another state, is a question that remains to be decided by the competent judicial authority.

3.3.3 The Law Applicable to the Protection of Personal Data

The account-based architecture, which requires access to the identity of the person holding the account, poses the additional risk of differing legal

protection concerning personal data. The right to have one's own personal data protected and not transferred is a personal right. Hence, it is conceivable that the national law – or the law of the habitual residence – of the holder of the account interferes in the payment operation. For instance, if a payor in country E pays in CBDC E to a beneficiary in country F and by receiving the payment, this beneficiary receives personal data that the debtor did not consent to give, because the law of protection of personal data in country F is less stringent than the law of country E, may the debtor claim the application of law E? An easy answer relies on the technology. If a payment can be made in CBDC E in country F, that means that country E and country F will have concluded an arrangement for the cross-border use of their CBDCs, which means that both central banks should have validated the level of data protection in the transfers. So the technology should nip the risk in the bud. But what happens if there's a "glitch?" Which law should apply? A clear conflict-of-laws rule solving this issue should be part of the legal toolkit that should accompany the issuance of CBDC.

3.4 *The Principle of Autonomy?*

A possible way through the complications arising from cross-border use of CBDC could be the automatic insertion of a choice-of-law clause in the algorithm. The expression "choice-of-law clause" is of course here figurative. If this possibility exists technically, the central bank will undoubtedly opt for the application of its own law, giving more and more importance to the *lex monetae* (*new formula*). We could also imagine a choice-of-forum-clause designating the jurisdiction of the state of the central bank, and why not, a dispute settlement clause which would refer to a particular mechanism to resolve the disputes related to the holding or transactions made with CBDC. The central bank could also put in place a specific arbitration mechanism, which would partly or totally function with artificial intelligence. But this is beyond the scope of this contribution.

4 Conclusion

In conclusion, we can assert two principles but have to leave many questions open. A first principle that seems certain for as long as states retain their monetary sovereignty is that the determination of the law applicable will remain an issue. In other words, we do not see any "global law" applicable to CBDC coming soon. A second principle is that the determination of the law applicable is closely linked to the pattern that will be chosen to develop cross-border payments with CBDC.

CHAPTER 13

The Law Applicable to Stablecoins

Matthias Lehmann and Hannes Meyle

1 Introduction

Stablecoins are increasingly popular crypto assets, with over 150 billion US$ of market capitalisation in the year 2021.[1] Like Bitcoin and other cryptocurrencies, stablecoins are recorded and transferred on digital ledgers. However, there is a crucial difference between them: Bitcoin is a so-called "native" crypto asset, without any intrinsic value and without any relation to an asset in the real or virtual world. By contrast, a stablecoin is commonly understood as a "cryptoasset that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets."[2] Such assets may be currencies, commodities, like precious metals or other traded goods, or even real estate. They can also be other digital assets, such as cryptocurrencies or investment tokens.

But stablecoins need not necessarily be backed by an asset – their "stability" can also be ensured via algorithms.[3] In this case, one speaks of "synthetic stablecoins". Also, stablecoins do not necessarily have a stable value in absolute terms, as it depends on their exact design how "stable" or risky they actually are.[4] The expression "stablecoin" therefore has the hallmarks of a marketing term.

1 See coincodex, "Stablecoins by Market Cap and Volume", <https://coincodex.com/cryptocurrencies/sector/stablecoins> accessed 18 February 2022); the Blockdata database (Blockdata, "Stablecoins list – A database of all stablecoin providers" (*Blockdata*) <https://www.blockdata.tech/markets/use-cases/stablecoins> accessed 18 February 2022); and the statista overview about market capitalization of the ten largest stablecoins (statista, "Market capitalization of the 10 biggest stablecoins from January 2017 to June 19, 2022" (*statista*) <https://www.statista.com/statistics/1255835/stablecoin-market-capitalization> accessed 18 February 2022).

2 Financial Stability Board (FSB), "Regulation, Supervision and Oversight of 'Global Stablecoin' Arrangements" (*FSB*, 13 October 2020), 5 <https://www.fsb.org/wp-content/uploads/P131020-3.pdf>.

3 See *infra* sub 2.4.

4 See for example the Swiss Financial Market Supervisory Authority (FINMA), "Supplement to the guidelines for enquiries regarding the regulatory framework for Initial Coin Offerings (ICOs)" (*FINMA*, 11 September 2019) <https://www.finma.ch/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-stable-coins.pdf>.

© MATTHIAS LEHMANN AND HANNES MEYLE, 2023 | DOI:10.1163/9789004514850_015
This is an open access chapter distributed under the terms of the CC BY-NC-ND 4.0 license.

In addition, the expression "stablecoins" is misleading because in reality most of them are not coins but tokens. The two terms are often used interchangeably but should be distinguished. The word "coin" designates crypto assets which have their own specific network; in contrast, tokens do not have a special protocol or network, but instead rely on a pre-existing network.[5] The latter is typically the case for stablecoins. A more appropriate expression would therefore be "stabletoken." Nevertheless, the designation as "stablecoins" is commonly used, which is the reason why it shall be used here as well.[6]

Possible design options and use cases for stablecoins vary considerably. Stablecoins that are linked to commodities facilitate global investments in assets that may otherwise be difficult to obtain or store, such as gold or oil. When pegged to a fiat currency, stablecoins are often seen as an alternative to traditional means of payment, without the disadvantage of strong fluctuation seen in other cryptocurrencies. Stablecoins can also allow for quick switches into other cryptocurrencies and back to stablecoins and are therefore commonly used to invest and secure profits from cryptocurrencies.

Supporters of stablecoins emphasise their potential to replace state-issued currencies with a seamless and more efficient payment system, which eliminates, or at least reduces, the role of intermediaries or centralised processes, such as risk-taking, decision-making, and record-keeping.[7] Critics point out their lack of safeguards and the danger of a run for the redemption of stablecoins, which may result in a token crash, as has happened in 2022 with the Terra/Luna debacle.[8] On a larger scale, such crashes may have very negative effects for the entire economy.[9] Particularly widespread – and at least partially founded – are complaints about the lack of transparency of stablecoins: Even for the most widely used stablecoin, Tether, there are still uncertainties regarding

5 Ke Wu, Spencer Wheatley and Didier Sornette, "Classification of Cryptocurrency Coins and Tokens by the Dynamics of Their Market Capitalizations" 5 (2018) Royal Society Open Science 180381, 2.

6 See also International Institute for the Unification of Private Law (UNIDROIT), "Digital Assets and Private Law Working Group, Issues Paper, Study LXXXII, W.G.3, Doc. 2 (rev. 1)" (*UNIDROIT*, June 2021), margin no. 57 <https://www.unidroit.org/english/documents/2021/study82/wg03/s-82-wg03-02-rev01-e.pdf> accessed 18 February 2022; FSB (n 3), 9.

7 Cf. Bank for International Settlement (BIS), "Stablecoins: risks, potential and regulation, BIS Working Papers No 905" (*BIS*, 24 November 2020) <https://www.bis.org/publ/work905.pdf>.

8 Financial Times, "Luna crash sends a chill through decentralised finance market" (*Financial Times*, 6 June 2022) <https://www.ft.com/content/c10bc6f7-abbe-45dc-9367-042186c3336f>.

9 BIS (n 7), 15 draws parallels to historical examples of banks creating their own private currency which led to high inflation and a debasement of the private bank currencies in circulation.

the financial assets held by the entity that issues the relevant tokens.[10] Another prominent example is the US-Dollar Coin (USDC), which was promised to be backed 1:1 by US-Dollars; nevertheless, this stablecoin has recently lost its peg to the dollar. In other words, it has "depegged".[11]

In general, and despite their shortcomings, stablecoins have been trusted by investors, who have turned them into an economic success story. Up to now, the main focus of legislators worldwide has been on regulatory questions.[12] Meanwhile, fundamental civil law questions have been left unresolved, in particular the question of how to qualify a stablecoin, and how to determine the relation between the stablecoin and its underlying asset. Considering the global nature of stablecoins, the answer depends on the applicable private law, which in turn is determined by rules of "conflict of laws" or Private International Law (PIL). The purpose of this chapter is to highlight the main issues

10 See for example Zeke Faux, "Anyone Seen Tether's Billions?" (*Bloomberg*, 7 October 2021) <https://www.bloomberg.com/news/features/2021-10-07/crypto-mystery-where-s-the-69-billion-backing-the-stablecoin-tether>; Matt Robinson and Bloomberg, "Cryptocurrency Tether is fined $41 million for lying about reserves" (*Bloomberg*, 15 October 2021) <https://fortune.com/2021/10/15/tether-crypto-stablecoin-fined-reserves>. Tether provided a report regarding its reserves, however it does not answer the question exhaustively. Tether, "Transparency" (*Tether*) <https://tether.to/wp-content/uploads/2021/08/tether_assuranceconsolidated_reserves_report_2021-06-30.pdf> accessed 18 February 2022.

11 See Ashley Capoot, "Stablecoin USDC breaks dollar peg after firm reveals it has $3.3 billion in SVB exposure", <https://www.cnbc.com/2023/03/11/stablecoin-usdc-breaks-dollar-peg-after-firm-reveals-it-has-3point3-billion-in-svb-exposure.html> accessed 10 April 2023.

12 See for example the International Organization of Securities Commissions (IOSCO), "Consultative report: Application of the Principles for Financial Market Infrastructures to stablecoin arrangements" (IOSCO, October 2021) <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD685.pdf> accessed 18 February 2022; Global Blockchain Business Council, "Global Standard Mapping Initiative (GSMI) 2020" (*GBBC*, October 2020) <https://gbbcouncil.org/wp-content/uploads/2020/10/GSMI-Legal-Regulatory-Report.pdf> accessed 18 February 2022; Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, [2020] COM/2020/593 final, 2020/265(COD); Swiss Federal Council, Rechtliche Grundlagen für Distributed Ledger-Technologie und Blockchain in der Schweiz – Eine Auslegeordnung mit Fokus auf dem Finanzsektor" (*Der Bundesrat*, 14 December 2018), 48 ff <https://www.newsd.admin.ch/newsd/message/attachments/55150.pdf> (Swiss DLT Report); see also the country reports available on the Legal 500, "Blockchain Guide" (*Legal500*) <https://www.legal500.com/guides/guide/blockchain/> accessed 18 February 2022. From the rich literature on regulatory questions regarding stablecoins, see *e.g.* Filippo Annunziata, "Speak, If You Can: What Are You? An Alternative Approach to the Qualification of Tokens and Initial Coin Offerings" (2020) 17 European Company and Financial Law Review 129; Anastasia Sotiropoulou, and Stéphanie Ligot, "Legal Challenges of Cryptocurrencies: Isn't It Time to Regulate the Intermediaries?" (2019) 16 European Company and Financial Law Review 652.

from a conflicts perspective, to examine to what extent these issues can be resolved with existing rules and principles, and to call attention to the need of new conflicts provisions that are tailored to this novel asset class.

2 Types and Use Cases of Stablecoins

To provide a solid base for the present analysis, first the functions and particularities of stablecoins need to be explained. This is not an easy task, as the term comprises "an incredibly mixed bag of things,"[13] and the structures of the underlying arrangements vary considerably. Most of them consist of several entities for the issuance and redemption of the token, as well as for its stabilisation, exchange, and the interaction with users.[14] Given their popularity, new types of stablecoins could be created in the future. Not all business models and constellations can be treated within the framework of this chapter. Instead, only basic and stylised use cases will be examined.

2.1 *Currency-linked Stablecoins*

By far the most common type of stablecoin is linked to one or several currencies.[15] To illustrate their functioning, the most widely used stablecoin, Tether, shall serve as example:[16]

One Tether token (USD₮) represents the value of 1 US$. When a Tether customer transfers 100 US$ to Tether Ltd., the latter puts 100 USD₮ into circulation by issuing them to the customer. The customer may use these USD₮s for trading, transfer them to other users as a means of payment, or hold them in a

13 UNIDROIT (n 6).

14 See for example HM Treasury, "UK regulatory approach to cryptoassets and stablecoins: Consultations and call for evidence" (*HM Treasury*, 7 January 2021), 6 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950206/HM_Treasury_Cryptoasset_and_Stablecoin_consultation.pdf>.

15 See for example the market capitalisation on CoinMarketCap (CoinMarketCap, "Top Stablecoin Tokens by Market Capitalization" (*CoinMarketCap*) <https://coinmarketcap.com/de/view/stablecoin/> accessed 18 February 2022. See also The Law Society and Tech London Advocates, "Blockchain: Legal & Regulatory Guidance, Second Edition" (*Azure Edge*, 2021), 69 <https://prdsitecore93.azureedge.net/-/media/files/topics/research/blockchain-legal-and-regulatory-guidance-second-edition-2022.pdf?rev=05e6855c881543a0b7b15a5a083bd828&hash=0DB718F58467B6162B0A3CDD30D10E1D> accessed 18 February 2022.

16 See the Tether FAQs (Tether, "FAQs" (*Tether*) <https://tether.to/en/faqs> accessed 18 February 2022) and the Tether Whitepaper (Tether, "Whitepaper" (*Tether*) <https://tether.to/en/whitepaper> accessed 18 February 2022) for details.

wallet. Upon the customers' request, the USD₮s will be redeemed, i.e., Tether Ltd. will pay 100 US$ to the customer. The outstanding tokens then either become part of Tether's "Treasury" or they are "burned." Tokens in the Treasury still exist on the blockchain, but they are out of circulation and therefore not part of the market capitalisation. Burned tokens are deleted and cannot be used anymore. This mechanism ensures that the number of USD₮ in circulation allegedly[17] equals the amount of US$ held by Tether and that the value of one USD₮ is stable relative to the US$.

Currency-linked stablecoins such as USD₮ can be used as means of payment provided that they are accepted by the other party. Some countries are considering introducing stablecoins as an official means of payment,[18] whereas others have tried to prevent private stablecoins from replacing fiat currencies[19] or submit them to tight conditions.[20] Where stablecoins meet the definition of "securities" or "electronic money" under national law, they will be covered by existing financial services legislation, but this does not entail a qualification for private (international) law purposes or an answer to the private (international) law questions they raise. From the perspective of token holders, it is crucial that the tokens are indeed backed up by financial assets if this has been promised, and that the investors can redeem tokens at the agreed rate. This requires not only a valid contract between token holder and issuer, but also a legally secure and enforceable connection between the token and the underlying assets.

17 However, Tether Ltd. might have made untrue or misleading statements regarding the reserves that actually back up USD₮; see the Commodity Futures Trading Commission, "Release Number 8450-21" (*CFTC*, 15 October 2021) <https://www.cftc.gov/PressRoom/PressReleases/8450-21>.

18 For example, the JP Morgan Coin has recently been tested by the Central Bank of Bahrain; see Central Bank of Bahrain, "Central Bank of Bahrain, Alba, Bank ABC and Onyx by J.P. Morgan Complete Test with Blockchain Based JPM Coin System" (*CBB*, 5 January 2022) <https://www.cbb.gov.bh/media-center/central-bank-of-bahrain-alba-bank-abc-and-onyx-by-j-p-morgan-complete-test-with-blockchain-based-jpm-coin-system>.

19 According to the German Ministry for Economics and Energy and the Ministry of Finance, "Blockchain-Strategie der Bundesregierung" (*BMWK*), no. 1.4 <https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/blockchain-strategie.pdf?__blob=publicationFile&v=8> accessed 18 February 2022, the German government wants to advocate at the European and international level that stablecoins do not become an alternative to state-issued currencies.

20 See the new Japanese regulation of stablecoins, Financial Times, "Japan passes stablecoin law giving protection to crypto investors" (*Financial Times*, 3 June 2022) <https://www.ft.com/content/7f8130e9-abfa-407b-b04f-2f9f5e47d0df>. See also the EU Proposal for a Regulation on Markets in Crypto-assets (MiCA), COM/2020/593 final.

2.2 *Stablecoins Linked to Real-worlds Assets*

Stablecoins may also be linked to tangible assets in the real world, such as land or commodities. One example that may serve as illustration for the present section is PAX Gold (PAXG):[21]

The PAXG token runs on the Ethereum blockchain and is issued by Paxos Trust Company LLC. Every PAXG token is backed by one troy ounce of gold; the customer may choose between allocated and unallocated gold.[22] Opting for allocated gold means that the customer becomes beneficial owner "of a pro rata portion" of a specific gold bar in a vault in London[23] and receives the serial number as well as information about the purity and the weight for each bar;[24] yet Paxos reserves itself the right to reallocate tokens to different bars.[25] When opting for unallocated gold, the customer does not become owner of specific gold bars but is entitled to a certain quantity of gold, which an institution promises to deliver. The prize of the tokens is pegged to the actual value of gold; in addition, Paxos charges certain fees for the issuance and administration of tokens.[26]

Tokenisation of commodities allows investment in and trading of assets that are only locally available or that require expensive storage. In most cases, and depending on the applicable threshold, the customer may redeem tokens into the underlying asset. The example of PAXG illustrates that asset-linked stablecoins have the potential to replace certain types of securities such as commodity futures, commodity forwards, or commodity-backed bonds. It also shows the importance of the goods underlying the token being linked to the stablecoin in a legally secure manner.

---

21 See the Paxos website (Paxos, "Pax Gold" (*Paxos*) <https://paxos.com/paxgold> accessed 18 February 2022).

22 One troy ounce (t oz) corresponds to roughly 31 grams; see Wikipedia, "Troy weight" <https://en.wikipedia.org/wiki/Troy_weight#Troy_ounce_(oz_t)> accessed 18 February 2022.

23 See Paxos, "PAX Gold Terms and Conditions" (*Paxos*), nos. 5.1–5.2 <https://paxos.com/2019/08/06/pax-gold-terms-conditions> accessed 18 February 2022.

24 *Id*. at no. 5.2.

25 *Id*.: "[…] in order to take into account transfers of PAXG tokens, new conversions of PAXG tokens, redemptions, and other PAXG transactional activity. This reallocation process will be automated and instantaneous, such that all PAXG tokens will be allocated to specific gold bars at all times."

26 *Id*. at no. 14: amongst others, fees on conversion, fees on transfer, storage fees, banking fees, and incentive fees.

2.3 *Stablecoins Linked to Cryptocurrencies*

Instead of currencies or commodities, tokens can also be linked to assets on other blockchains. For example, Wrapped Bitcoin (WBTC) is a stablecoin backed 1:1 with bitcoins, which can be used on other blockchains than the Bitcoin network.[27] Third parties act as custodians, and there is an openly accessible list of public keys where the bitcoins held can be verified. This arrangement has the benefit of being transparent. It allows to extend the use of bitcoin to technical functions not available on the original Bitcoin network.

2.4 *Algorithmic Stablecoins*

Another possibility is to maintain the value of stablecoins by means of algorithms, in particular smart contracts. An example of this type of "algorithmic stablecoin" was Luna, which spectacularly crashed in 2022.[28] A further illustration is Dai, a stablecoin that is issued by the MakerDAO. Dai is "soft-pegged" to the US dollar; its stability is guaranteed by the use of specialised algorithms and smart contracts that manage the supply of tokens in circulation.[29] The goal of such a system is to keep the value of the token close to a reference asset such as the US dollar and to buffer against price fluctuations. For example, when the market price of the token falls below the value of the tracked currency, the algorithmic stablecoin system will reduce the number of tokens in circulation, whereas new tokens will be issued when the price of the token exceeds the price of the tracked currency.[30]

Stablecoins of the algorithmic type are not linked to another asset and therefore do not raise any particular questions of PIL that would be different from those of crypto assets in general. Therefore, the present chapter will not treat them any further.

2.5 *Interim Conclusion*

While the use cases vary, the basic constellation of stablecoins can be summarised as follows: upon payment or in exchange for other assets, the customer

---

27 See Wrapped Bitcoin, "Do More With Your Bitcoin" (*WBTC*) <https://wbtc.network> accessed 18 February 2022.

28 See *supra* n 8.

29 See MakerDAO, "The Maker Protocol> MakerDAO's Multi-Collateral Dai (MCD) System" (*MakerDAO*) <https://makerdao.com/en/whitepaper#abstract> accessed 18 February 2022.

30 See the entry in the encyclopedia by Gemini, a crypto exchange and custodian provider (Cryptopedia, "What Are Stablecoins?" (*Gemini*, 28 June 2022) <https://www.gemini.com/cryptopedia/what-are-stablecoins-how-do-they-work#section-crypto-collateral-on-chain>.

receives tokens which are typically issued and redeemed by a central authority – in contrast to cryptocurrencies such as Bitcoin which are regularly issued in a decentralised way and never redeemed. The value of the token is linked to an underlying asset, which can be either an off-chain asset or a "native" asset, i.e. one that itself exists only on the blockchain. The rights of the token holder with regard to the underlying asset depend on the exact design of the stablecoin. For example, some terms and conditions provide that the token holder becomes owner of a specific underlying asset (*e.g.* PAXG allocated), while others provide for a contractual claim on a type of asset (*e.g.* USD₮, PAXG unallocated), and still others rely on technological solutions (*e.g.* WBTC). In order to function, all asset-backed stablecoins require a legally secure connection between the token and the underlying asset.

3. Stablecoins and Substantive Law

The purpose of this chapter is to address issues of global PIL, in particular to develop autonomous connection factors. However, PIL can never be completely detached from the substantive law level, which determines whether and how stablecoin arrangements work. The challenge is that the substantive law regarding stablecoins is still evolving.[31] Therefore, we are not yet in a position to provide a conclusive summary of the legal landscape of distributed ledger technology. However, it is already possible to identify trends in substantive law that may have an influence on PIL.

3.1 *Switzerland*

In 2021, Switzerland adopted the Federal Law on the Adaptation to Developments in the Technology of Distributed Electronic Registers, which amended several existing laws, including the Swiss Code of Obligations (OR) and the Swiss Federal Private International Law Act (PILA). As a result of the reform, rights that can take the form of traditional securities may now also be represented by ledger-based securities ("Registerwertrechte," "droits-valeurs

31 See the overview provided by the Hague Conference HCCH, "Developments with respect to PIL implications of the Digital Economy: Document Prel. Doc. No 4 of December 2021" (*HCCH*, March 2022), 16 ff <https://assets.hcch.net/docs/137199d5-4bc2-42b7-93ab-d97a3b8a6d60.pdf> accessed 31 July 2022. For a comparison of private law initiatives in France, Liechtenstein, the UK, and the USA see Matthias Lehmann, "National Blockchain Laws as a Threat to Capital Markets Integration" (2021) 26 Uniform Law Review 148.

enregistrés," "diritti valori registrati").[32] This covers, for example, claims, stock corporation membership rights, and mortgage certificates (*Schuldbriefe*, Art. 842 Swiss Civil Code).[33] It also applies to stablecoin tokens.[34]

The new Swiss law does not contain specific rules regarding the qualification and legal effects of tokens as such. Art. 973f OR merely gives effect to the rules of the register. According to the legislative materials, the transfer of tokens follows the principles of property law and is subject to a valid underlying transaction.[35] The new provisions contain similarly general conditions for the creation,[36] effects,[37] collateralisation,[38] and cancellation[39] of ledger-based securities, as well as rules on information duties and liability[40] relating to them.

There are no special provisions on asset securitisation in the new law. In particular, ownership of an underlying asset cannot be transferred directly with a token. However, insofar as a token is underpinned by a possession assignment or similar arrangement ("Besitzanweisungsvertrag"; "Besitzkonstitut"), the token transfer can be considered as a transfer of possession regarding the asset and thus as one of the necessary elements of a transfer of ownership in the asset.[41] This construction would allow the operation of a stablecoin under Swiss law.

---

32 See Swiss Federal Council, "Botschaft zum Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register)" (*Fedlex*, 27 November 2019), 276 <https://www.fedlex.admin.ch/eli/fga/2020/16/de>.

33 Swiss DLT Report (n 12), 68.

34 Swiss Federal Council (n 32).

35 *Id*. at 286: "The details of the transfer differ depending on the registry and namely on the consensus mechanism chosen. It is crucial that the registration agreement is transparent on this point (Art. 973d par. 2 No. 3 E-OR). The Federal Council assumes that the transfer of the ledger-based security - analogous to the transfer of a security which it emulates – is in principle causal to its underlying transaction. Many – though not all – participants in the consultation procedure shared this view. Thus, for a valid transfer, a valid contractual agreement (e.g. a purchase) is required as well as the actual transfer in the register as conveyance of title".

36 Art. 973d OR.

37 Art. 973e OR.

38 Art. 973f OR.

39 Art. 973h OR.

40 Art. 973i OR.

41 *Id*. at 66: "[o]n the one hand, where a transfer of the token equals a transfer of actual control over the thing, ownership of the thing may be transferred in this way. Use cases of this mechanism could be so-called smart property. On the other hand, where ownership and direct possession do not coincide, a transfer by means of an informal possession assignment contract or a possession constitute ('Besitzkonstitut') is possible. The will to transfer indirect possession may also be expressed by moving a token. If the blockchain is public or can at least be viewed by the direct possessor of the thing, displacement of the

3.2 *Liechtenstein*

The Principality of Liechtenstein adopted legislation in 2019 in the form of the Law on Tokens and Service Providers of Trusted Technologies ("Token- und VT-Dienstleister-Gesetz," TVTG).[42] Liechtenstein also introduced the new legal term of so-called book-entry securities ("Wertrechte"), which covers certain stablecoins.[43] In principle, features and functions of a physical certificate are replaced by the tokens as entries in a digital ledger.

As regards the qualification of tokens, the Liechtenstein legislator does not use the notion of ownership to describe the relation between a token holder and the token. Instead, Art. 5(1) TVTG specifies that the Trustworthy Technology key holder "has the power of disposal over the token." According to Art. 4 TVTG, tokens are considered to be "patrimony" located in Liechtenstein.[44] Art. 5 ff. TVTG establish specific conditions for the right of disposal, transfer, and good-faith acquisition of tokens. One particularly noteworthy aspect of Liechtenstein law is that it requires a separate contract, similar to a transfer of property under German law.[45] This means that a legally valid token transfer does not depend on the validity of the underlying contractual obligation to transfer. This constitutes a stark contrast to the principles of Liechtenstein property law, which is otherwise based on the causality principle.[46]

The legislative materials correctly state that coordinating the transfer of a digital token and the transfer of a real-life asset is the central challenge when regulating tokens from a private law perspective.[47] The corresponding basic

---

token can at the same time serve as an indication to the direct possessor to know that he now possesses for a new owner".

42 Gesetz vom 3. Oktober 2019 über Token und VT-Dienstleister (Token- und VT-Dienstle ister-Gesetz; TVTG), 2019.301 (available online at <https://www.gesetze.li/konso/2019 301000>) ("TVTG").

43 See Gesetz vom 3. Oktober 2019 über die Abänderung des Personen- und Gesellschafts-rechts, 2019.304, § 81a SchIT (available online at <https://www.gesetze.li/chrono /2019304000>).

44 In the original: "gilt der Token als im Inland befindliches Vermögen", Art. 4 TVTG.

45 TVTG (n 42), Art. 6(2); see in detail Lehmann (n 31), 159 f.

46 See Daniel Damjanovic, Vanessa Pfurtscheller, and Nicolas Raschauer, "Liechtensteins 'Blockchain Regulierung' – Ein- und Ausblicke" (2021) 2 Zeitschrift für Europäisches Privatrecht 397, 411. For practical problems that may arise when the principle of abstraction is applied in the context of blockchain transactions, see Lehmann (n 31), 159 f.

47 Report of the Government Liechtenstein, "Bericht und Antrag der Regierung an den Landtag des Fürstentums Liechtenstein betreffend die Schaffung eines Gesetzes über Token und VT-Dienstleister", Nr. 54/2019, 63 f. (available online at <https://bua.regierung.li/BuA/dynamic_bridge.jsp?buajahr=2019&buanr=54>): "Online legal certainty means that the acquirer of a token must be certain that he is also acquiring the right associated with the token. Offline legal certainty means that persons who acquire a thing or a right in the offline-world must not be exposed to the risk of coming away empty-handed in relation

rules are laid down in Art. 7 TVTG. They are noteworthy in particular because they illustrate the substantive-law connection: According to Art. 7(1) TVTG, a disposal over the token results in the disposal over the right represented by the token. If this legal effect does not come into force by law, according to Art. 7(2) TVTG, the person obliged to transfer the token must ensure that the disposal over a token directly or indirectly results in the transfer of the represented right, and that a competing disposal over the represented right is excluded. As the "right" can relate to anything, including participations in companies or rights *in rem*, a stablecoin can well be a token in the sense of the TVTG.

3.3 *Germany*

In 2021, Germany adopted the Electronic Securities Act (eWpG) in order to ensure the legal protection of electronic securities such as crypto negotiable instruments ("Kryptowertpapiere").[48] As regards the type of security, the law mainly covers bearer bonds (*Inhaberschuldverschreibungen*) and some types of investment fund participation.[49] The Act also includes German covered bonds (*Pfandbriefe*), i.e. negotiable instruments backed up by other assets, such as mortgages. This inclusion of covered bonds could provide a basis for introducing a stablecoin governed by German law.

Sec. 2(3) eWpG provides that electronic securities are deemed to be things in the sense of Sec. 90 German Civil Code (BGB), which are defined as "corporeal objects" and are the basis of the German "law of things" (*Sachenrecht*), or property law. Sec. 2(3) eWpG subjects electronic securities to the rules on property law as laid out in Book 3 of the BGB. It follows that these assets are considered as the subject of property rights in insolvency proceedings and

---

to acquirers of corresponding tokens. Both requirements – legal certainty online and offline – are mandatory conditions for a legal framework designed to enable the transfer of assets. Legal certainty online can be ensured by the TVTG stipulating that the disposition of a token simultaneously effects conveyance of the represented right. In the interest of legal certainty and clarity, it also needs to be clear for the individual categories of assets that can be represented (things, receivables, etc.) that disposal by means of tokens is possible. However, such a clarification in a Liechtenstein law can only have effect for assets that are subject to Liechtenstein law (e.g. a movable property located in Liechtenstein)." I*d.* at 168.

48 German Government Bill of an Act for the Introduction of Electronic Negotiable Paper ("Gesetzentwurf der Bundesregierung zum Entwurf eines Gesetzes zur Einführung von elektronischen Wertpapieren"), 24 February 2021 BT-Drs. 19/26925, 1 (available online at <https://dserver.bundestag.de/btd/19/269/1926925.pdf>).

49 German Act on Electronic Securities (Gesetzes zur Einführung von elektronischen Wertpapieren vom 3. Juni 2021 (BGBL. I S. 1423) ("eWpG"), Sec. 1; see also German Government Bill of an Act for the Introduction of Electronic Negotiable Paper (n 48), 56.

enjoy corresponding protection.[50] The underlying idea of the German legislator was to not create *sui generis* rights, but to apply existing rules as far as possible.[51]

Insofar as crypto rights are created, however, the new Act contains some special rules that deviate from the general rules of property law, which are geared towards tangible (corporeal) assets. In particular, the connection between token and underlying asset is governed by Sec. 25 eWpG, which specifies that the right following from the token is transferred by transferring the ownership of the token.[52] This could be a basis for the transfer of rights and obligations resulting from stablecoins, assuming that a covered bond will be arranged for this purpose.

3.4 *Common Law Countries*

According to the UK Jurisdiction Taskforce, crypto assets are "sufficiently permanent or stable to be treated as property" and "possess all the characteristics of property set out in the authorities" under Common law.[53] Courts in several countries have confirmed that tokens and other crypto assets may qualify as property objects.[54]

In the US, property law and property protection are not part of federal legislation, but within the competence of the individual states. The Uniform Regulation of Virtual-Currency Businesses Act (URVCBA) tries to harmonise the law of the federal states, but mainly from a regulatory viewpoint.[55] The Uniform

50 Michael F. Müller and Christian Pieper, "§ 2" in Michael F. Müller, Christian Pieper, and Bernhard Barth (eds), *eWpG: Gesetz über elektronische Wertpapiere* (C.H. Beck 2022), para. 19; German Government Bill of an Act for the Introduction of Electronic Negotiable Paper (n 48), 40.

51 German Government Bill of an Act for the Introduction of Electronic Negotiable Paper (n 48), 39.

52 See eWpG (n 47), sec. 25: "(1) In order to transfer ownership of an electronic security, the electronic security must be transcribed to the transferee upon instruction of the beneficiary and both parties must agree that ownership is to be transferred. Before the transcription to the name of the transferee is carried out, the beneficiary does not lose ownership. (2) The right following from the security is transferred with the transfer of ownership of the electronic security according to paragraph 1".

53 UK Jurisdiction Taskforce, "Legal Statement on Cryptoassets and Smart Contracts" (*Tech Nation*, 2019), 16, margin nos. 56 f <https://technation.io/lawtech-uk-resources/#gf_41> accessed 18 February 2022.

54 See the Summary of Selected Case Law in HCCH (n 31), Annex III, with examples from New Zealand, Singapore, the UK, Shanghai, and Canada (British Columbia).

55 Uniform Law Commission, "Uniform Regulation of Virtual-Currency Businesses Act" (*ULC*) https://www.uniformlaws.org/viewdocument/final-act-154?CommunityKey=e104aaa8-c10f-45a7-a34a-0423c2106778&tab=librarydocuments accessed 3 December 2021. On the URVCBA, see *e.g.* Lehmann (n 31), 162 ff.

Supplemental Law (USL) on the URVCBA also addresses private law issues.[56] It treats digital currencies in the same way as securities and provides the holder with a "securities entitlement." The Act is not a major success so far, as it has been adopted only by Rhode Island.[57] Some states have consciously deviated from the USL on the URVCBA and granted property protection for tokens, *e.g.* Wyoming.[58] These differences of legal rules create frictions even within the USA.

Regarding stablecoins, as far as can be seen, there is no legislation or court decision explicitly addressing their status under private law. In particular, the relationship between the token and the underlying asset remains subject to considerable uncertainty. Common law jurisdictions thus do not provide at the moment a stable legal environment for stablecoins.

3.5 *Conclusion*

Stablecoins are a moving target because legislation is still evolving. Some countries have already addressed substantive law questions. One tendency seems to be to treat stablecoins similar to securities, provided that they embody the same rights. The fact that countries like Switzerland and Liechtenstein, with strong financial sectors, follow this approach might have a signaling effect for other countries.

For the moment, legislators mostly deal with currency-linked and commodity-linked stablecoins, which are the most widely used, whereas stablecoins linked to on-ledger assets or managed by algorithms have yet been spared.[59] Also, all legislative projects assume that there is a central body that issues and manages tokens and is responsible for providing accurate information about them. Many regulations, for instance the German law, focus on so-called permissioned blockchains, i.e. one with a central operator that administrates the network and is under state supervision. In this case, the issuer may be the same person as the central operator, or a different one. However, some laws do not necessarily require a permissioned blockchain, *e.g.* those of Liechtenstein

56 Uniform Law Commission, "Supplemental Commercial Law for the Uniform Regulation of Virtual Currency Businesses Act" (*ULC*) <https://www.uniformlaws.org/viewdocument/enactment-kit-48> accessed 3 December 2020.

57 See the enactment history on Uniform Law Commission, "Regulation of Virtual-Currency Businesses Act" (*ULC*) <https://www.uniformlaws.org/committees/community-home?CommunityKey=e104aaa8-c10f-45a7-a34a-0423c2106778> accessed 31 March 2022.

58 Wyoming Bill no. SF0125, LSO no.: 19LSO-0608, Enrolled Act no.: SEA no. 0039, Wyoming Statutes (W.S.) 3429101 ff.

59 See for example the Report of the Government Liechtenstein (n 47), 65.

and Switzerland. Under these laws, it is possible to issue the token on a permissionless blockchain, i.e. one that is completely decentralised. The rules that apply in this case will be the same as for a permissioned blockchain.

In sum, national rules on stablecoins vary greatly in detail, which represents an obstacle for stablecoins as a global business model. Against this background, legislators and international stakeholders should aim for a uniform private law for the blockchain.[60] As this is an ambitious long-term goal, legal certainty and predictability should be provided at least to the maximum amount on a PIL level. In order to archive this goal, connecting factors must be found that protect the legitimate expectations of stablecoin investors.

4 Stablecoins and PIL

Because of the complexity of the arrangement and the multiple relations involved, stablecoins present particular challenges when it comes to the identification of the governing law through PIL rules. A PIL analysis must start with a characterisation of the legal relationship in order to identify the correct conflicts rules. The challenge with stablecoins is that there is no international consensus about their characterisation on the substantive law level and even less regarding their characterisation for PIL purposes. Nevertheless, some fundamental distinctions can be drawn.

First, it is important to distinguish between (1) the law that applies to the contractual relationship between the issuer and the token holder and (2) the law that applies to the relationship between the token holder and other parties who compete over the stablecoin and/or the underlying assets. The latter relationship is considered as governed by property or patrimonial law in many jurisdictions, a characterisation that should also be followed on the conflicts level.

We will first discuss the law that applies to the relation between the issuer and the stablecoin token holder (4.1.). After that, we will address the proprietary or patrimonial issues. We will initially analyse them regarding the stablecoin (4.2.), followed by a discussion of the law that applies to the underlying assets (4.3.) and the law that governs the relation between the asset and the stablecoin (4.4.). It is in the last area (4.5.) that stablecoins present particularities distinguishing them from other coins or tokens.

60 Lehmann (n 31), 167 ff., 171; see also in this regard UNIDROIT (n 6).

4.1 *Law Applicable to Contractual Relationship between Issuer and Token Holder*

Stablecoins may be redeemable for an underlying fiat currency, for commodities, or other assets, pursuant to the issuer's general conditions. Regardless of the type and detail of the respective stablecoin, this relationship between token holder and token issuer is of a contractual nature. Some of the larger stablecoin issuers have stipulated choice-of-law clauses in their general terms and conditions: Some have opted for the law in force at their seat, others for the law of states known to be home to off-shore companies.[61] In comparison to property law, where a choice of law is typically not possible, PIL rules for contract law are generally open to party autonomy. This raises the question of how much room is left for a choice of law by the parties and what the scope of choice-of-law clauses would be.

Party autonomy is a fundamental principle in PIL.[62] Therefore, in many systems of PIL, the contracting parties are, in principle, free to choose the law applicable to their contractual relationship.[63] In the US,[64] this freedom is limited in particular by the Restatement (Second) of Conflict of Laws § 187(2)(a), which requires a "substantial relationship" of the law chosen to the parties or the transaction. In addition, an express choice of law by the parties will not be given effect if the application of that law "would be contrary to a fundamental

61 See e.g. the Tether General Terms and Conditions (GTC), sec. 1.4 of which provides for an arbitration clause and choice of law in favor of the British Virgin Islands (Tether, "Gold Token Terms of Sale and Service" (*Tether*, last updated 23 March 2022) <https://gold.tether.to/legal/termsofservice>; the Binance GTC contain an arbitration clause, a class action waiver, and a choice of Hong Kong law (Binance, "Binance Terms of Use" (*Binance*, last revised 12 July 2022) <https://www.binance.com/en/terms>); the TrueUSD Terms of Service provide for an arbitration clause and a choice of British Virgin Islands law (TrueUSD, "TRUEUSD TERMS OF SERVICE" (*TrueUSD*, last modified 2 February 2021) <https://trueusd.com/terms-of-service>).

62 Horatia Muir Watt, "Party Autonomy," in Jürgen Basedow et al. (eds), *Encyclopedia of Private International Law,* vol 2 (Cheltenham: Edward Elgar Publishing 2017), 1336 ff.; Giesela Rühl, "Private International Law, Foundations," in id., 1383: "traditional core of private international law".

63 Jürgen Basedow, "Choice of law," in Jürgen Basedow et al. (eds), *Encyclopedia of Private International Law* (n 62), 311 ff.

64 Note that there are no unified choice of law rules in the US because the individual states have their own choice-of-law regime. See Linda Silberman, "Country Report USA," in Jürgen Basedow et al. (eds), *Encyclopedia of Private International Law* (n 62) vol *3*, 2642. But nowadays US courts principally "permit party autonomy with respect to the applicable law in contracts and other transactions." see *id.* at 2643.

policy" of the state whose law would otherwise have been applied under the Restatement (Second) of Conflict of Laws.[65]

In Europe, the freedom of choice is even more pronounced:[66] According to Art. 3 Rome I Regulation, contractual parties are free to choose and change the law applicable to the contract, for parts of the contract or for the contract as a whole. In Swiss PIL, Art. 116(1) PILA simply states that "[c]ontracts are governed by the law chosen by the parties."

There may be limited effects to the choice of law by the parties under the law of the European Union in the event that a law having no connection to the contract is chosen.[67] The same applies if a weaker party is involved. Specifically, consumer protection rules curtail the free choice of law in the EU by maintaining the protection by the mandatory rules at the consumer's habitual residence (see Art. 6(2) Rome I Regulation). This is because the EU follows a very wide definition of consumer contracts, which covers every agreement that is made for a purpose outside the trade or profession of one party, provided that the other party exercises its commercial or professional activity in the country of the habitual residence of the consumer or directs it there (Art. 6(1) Rome I Regulation).

Other countries, such as Switzerland, exclude the choice of law in consumer contracts altogether (Art. 120(2) Swiss PILA). At the same time, however, Swiss law, like many other laws, has a more limited definition of "consumer contracts", restricting it to agreements for personal or family use (Art. 120(1) Swiss PILA).[68] This does not include investment contracts above a certain threshold.

---

65 The American Law Institute, "Restatement (Second) of Conflict of Laws" (*ALI*, 1971) <http://www.kentlaw.edu/perritt/conflicts/rest187.html> accessed 18 February 2022; on § 187, see Silberman (n 64), 2643.

66 See in particular Rome I Regulation (Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), [2008] OJ L177/6), Art. 3; Swiss Federal Act on Private International Law of 18 December 1987 (PILA), AS 1988 1776, SR 291, Art. 116.

67 See Rome I Regulation (n 65), Art. 3, paras. 3 and 4: "3. Where all other elements relevant to the situation at the time of the choice are located in a country other than the country whose law has been chosen, the choice of the parties shall not prejudice the application of provisions of the law of that other country which cannot be derogated from by agreement. 4. Where all other elements relevant to the situation at the time of the choice are located in one or more Member States, the parties' choice of applicable law other than that of a Member State shall not prejudice the application of provisions of Community law, where appropriate as implemented in the Member State of the forum, which cannot be derogated from by agreement".

68 For the interpretation of this notion in Swiss substantive law see Swiss Federal Tribunal, decision of 23 February 2005, 4C 292/2005, BGE 132 III 269, 273; decision of 8 February 2008, 4A 432/2007.

A contract over stablecoins of a considerable value (in the range above 80.000 CHF) would therefore not fall under the consumer protection provision, and the applicable law could be freely chosen.

4.2 *Law Applicable to Proprietary Questions of Stablecoin Tokens*

From a functional perspective, all stablecoin tokens share the same nature as other digital assets.[69] Even though there might be differences from a regulatory perspective,[70] the starting point for the determination of the applicable private law rules should thus be the same for all kinds of digital assets. Moreover, their holders have the same interests as those of any other asset – they want title and ownership to be recognised by everyone and not just by certain persons; they want to be free to sell, transfer, gift, or keep the token; and they want the right to claim back tokens taken from them without authorisation.[71] They also want as much protection as possible in case of the insolvency of an intermediary.[72] The question of who has title, power of disposal, or "ownership" over the token, i.e. the digital asset, is functionally fulfilled by the rules of property law, which suggests treating digital assets in the same way as corporeal assets. As shown above, this view is shared by an increasing number of courts and legislators (see *supra* sub 3). The UNIDROIT Working Group on Digital Assets and Private Law is moving in the same direction and proposes that "digital assets may be the subject of proprietary interests."[73]

However, the basic question whether tokens are subject to property law is not answered conclusively.[74] Some national legal systems may adopt a different characterization on the grounds of the intangible nature of tokens.[75] Civil law codifications generally provide for rigid definitions of the possible objects of property rights, as opposed to the more flexible and contextual approach of

69 For the scope of the term "digital assets," see UNIDROIT (n 6), 13 ff.

70 On these differences see, *e.g.*, The Law Society and Tech London Advocates (n 15), 48: "[i]t is noteworthy that stablecoins do not have their own category under the FCA taxonomy. This is because stablecoins may be structured in different ways, leading to different regulatory treatment. For example, in its Final Guidance on Cryptoassets, the FCA indicates that stablecoins could be regulated as e-money, as units in a collective investment scheme or another type of security token, or could fall outside the UK regulatory perimeter, depending on the way they are structured, their stabilization mechanism and other substantive characteristics".

71 See Jason G. Allen, "Property in Digital Coins" (2019) 8 European Property Law Journal 64, 69 on practical issues with the legal treatment of tokens.

72 See Lehmann (n 31), 157.

73 UNIDROIT (n 6), 16.

74 Allen (n 71), 70 draws parallels to data in general.

75 This seems to be the case under Japanese law; see *infra* the contribution on Japanese law by Tetsuo Morishita.

the Common law.[76] It is not excluded that certain legal systems will create new categories of ownership or property for the novel assets.[77] For example, the UK Law Commission is evaluating whether certain digital assets should be categorised as "belonging to a third category of personal property which is neither a thing in action nor a thing in possession" to reflect the particular features of digital assets more accurately under the Common law.[78]

Therefore, the final determination of the legal nature of stablecoins is left to the law governing them. However, such national characterisations should not predetermine the conflicts rules to be followed. Otherwise, the applicable law could not be determined in the same way, and forum shopping would be encouraged. Thus, it is vital to find a universal PIL category and a universal connecting factor for stablecoins.

4.2.1 *Lex Rei Sitae*

The fictional treatment of tokens as corporeal objects,[79] which is followed by some legislators on the level of substantive law, would, in principle, result in the application of the *lex rei sitae* rule on the conflicts level.[80] Accordingly, rights or entitlement in digital assets would be governed by the law of the place at which the property is situated. However, applying this rule to stablecoins is not practical, as it is nearly impossible to determine the situs of an asset held on a digital ledger,[81] given that one of the most important features of digital ledger technologies is their decentralisation. A token on a permissionless distributed ledger is located everywhere because it is stored on all the nodes of the relevant network, and at the same time it is located nowhere because no single node is authoritative or dispositive of its existence.[82] Typically, there is not even a central server that could be used as physical connecting factor. This goes to show why the location of a token cannot be transposed from the digital into the real world.

---

76 Lehmann (n 31), 152; Allen (n 71), 71.

77 Allen (n 71), 87.

78 The Law Commission, "Digital Assets Interim Update, 24 November 2021" (*Law Commission*), 3 f. <https://www.lawcom.gov.uk/project/digital-assets> accessed 18 February 2022.

79 See for example on German law *supra* sub 3.3.

80 Note, however, that even the German legislature, despite treating crypto assets as tangible property, does not draw the conclusion that the coins would be subject to the *lex rei sitae* principle. Instead, it opts for the law of the country in which the network is supervised, see eWpG (n 47), sec. 32.

81 See also the Financial Markets Law Committee (FMLC), "Distributed Ledger Technology and Governing Law: Issues of Legal Uncertainty" (*FMLC*, March 2018), 10 <http://fmlc.org/wp-content/uploads/2018/05/dlt_paper.pdf > accessed 18 February 2022.

82 Allen (n 71), 77.

4.2.2 Connecting Factors for Other Intangible Assets

Traditional intangible assets like copyrights, patents, trademarks, and other intellectual property rights pose similar challenges. However, no general conflicts rule has been established in their regard so far. There are only fragmentary rules and abstract principles like the territoriality of intellectual property rights, which do not lend themselves for tokens on a blockchain. Thus, it is possible that a separate conflict-of-laws rule needs to be devised for digital assets, in particular for those recorded on a blockchain. A general rule of PIL to answer the question of the applicable law to them is still missing.[83] Considering the decentralised nature of stablecoins, it is questionable whether a rule can be found that identifies a connecting factor with regard to them. Instead, it seems more promising to establish rules that refer to the participants to a blockchain.

4.2.3 Primary Residence of the Issuer

Since the purpose of a blockchain is to process transactions on a global level under the conditions of pseudonimity, it does not seem promising to try to locate the individual persons holding the tokens as long as there are other participants. Instead, the focus should be on the provider side.

In this regard, the issuer of the stablecoin is of prime importance. The issuer is the person who offers the token to the public.[84] This person must be distinguished from the generator, which takes care of the technical details of the issuance.[85] The two activities can be carried out by the same entity, but do not necessarily coincide.[86] It is important to distinguish between them, because it is only the issuer that takes legal responsibility for the issuance.

In terms of PIL, the issuer of a stablecoin is a useful connecting factor because the issuer is most often known. For instance, the issuer of Tether is Tether Limited, a company incorporated and based in Hong Kong.[87]

Focusing on the issuer of the stablecoin has a crucial advantage: It limits the number of possible applicable laws. All transfers of the stablecoin issued by a certain issuer are subject to the same rules. This creates legal certainty and prevents legal fragmentation. Thus, the issuer should be retained as a subsidiary criterion in the absence of a choice of law. More specifically, the applicable law should be that in force at the principal place of business of the issuer. Where the latter is not known, it should be the issuer's place of incorporation.

---

83 See e.g. Swiss DLT Report (n 11); Matthias Lehmann, "Who Owns Bitcoin? Private Law Facing the Blockchain" (2019) 21 Minnesota Journal of Law, Science & Technology 93, 93–136.

84 See TVTG (n 42) Art. 2 para. 1 lit. k.

85 *Id*. at Art. 2 para. 1 lit. l.

86 Report of the Government Liechtenstein (n 47), 153.

87 See Tether, "WhitePaper" (n 16).

4.2.4 Place of the Validator

For those stablecoins for which the issuer or its place of incorporation or principal place of business cannot be determined, another solution must be found. In the context of stablecoins that are backed by real-word assets such as currencies or commodities, there is often a so-called validator whose task it is to conclude the necessary arrangements regarding the collateral.[88] The validator manages and supervises the composition of the portfolio that backs the stablecoin. As investments in stablecoins increase, these validators will also be subject to increased regulation. This means that in the future it will likely be mandatory that the issuers of stablecoins indicate a relevant validator as the contact point for regulators and as the entity that is accountable for regulatory compliance. There may be another legal or natural person that enters contracts for the assets, and further persons that perform different services and activities around them.

This makes the definition of the relevant persons difficult. For example, the Liechtenstein TVTG distinguishes between no less than eleven different service providers or agents that must apply to be entered into a service provider register if their headquarters or place of residence is in Liechtenstein. Further, there might be doubts about who performs the functions of the validator. There might also be situations where there are several administrators with equal powers which makes it difficult to determine the relevant one.

Other problematic cases could arise because the place of the validator is not a permanent fixed connecting factor, but subject to change. For example, the relevant validator may move to another location. However, in this regard, the establishment of the validator is not more problematic as a connecting factor than the habitual residence of a natural person or the "real" seat of a legal person. Where important responsibilities are assumed by several entities, criteria need to be found to determine the relevant validator to determine the applicable law. Ideally, this person or entity should be the same entity as the contact point for regulatory purposes. This is only possible if regulatory and PIL rules are coordinated on at least a country level. On a global level, such coordination might be difficult to achieve, as every country has an interest in determining the most accessible contact point for regulatory compliance. This means that possibilities for forum shopping might arise.

4.2.5 Other Criteria

Where neither the issuer nor the validator are known, another option would be to look at the person in charge of the technical aspects of the DLT network on which the stablecoin is issued.

88 Report of the Government Liechtenstein (n 47), 72 ff.

Some distributed ledger systems function with a master key, by which the ability to transfer a digital asset is ultimately controlled. It has been suggested to use the primary residence, center of main interests, or, possibly, the domicile of the master key-holder as a connecting factor to identify the law applicable to property issues over digital assets (so-called Primary Residence of the Encryption Private Master Keyholder, or "PREMA").[89] However, this solution has a crucial disadvantage: There are only few systems which have master keys. Another disadvantage is that the location of the master key can change and is not transparent to third parties. Even though this connecting factor has the theoretical advantage of being unitary, it does not seem useful as a connecting factor.

As a default rule, it has also been proposed to use the place of the relevant operating authority (PROPA).[90] Such an operating authority exists on permissioned blockchains. For permissionless blockchains such as Ethereum, this criterion does not work. In these cases, one could try to localise the protocol under which the particular stablecoins have been issued. For instance, one might refer to the company that has created the protocol to determine its most significant connection and then transfer this connecting factor to all stablecoins that have been issued using this protocol. Of course, this is a residuary criterion, which applies only where an applicable law has not been chosen or the identity and location of the issuer and validator are unknown.

4.2.6 Party Autonomy?

To overcome the localisation problems of stablecoins, one might think about the participants to a blockchain to freely select the law governing proprietary rights regarding the digital assets recorded on the blockchain.[91] There are fundamental objections against free choice of law in the area of property law, in particular the effects property rights and other rights *in rem* have against third parties who have not consented to the choice of law and potentially do not even have knowledge of the law chosen.[92] These arguments do not carry the same force, however, in a network like the blockchain where parties have to consciously enter and could be required to consent, at this moment, to a law that has been chosen by the creators to govern the whole network. Yet such a

89 FMLC (n 81), 18 f.

90 See in particular *id.* at 18.

91 On free choice of law regarding the relation between the stablecoin issuer and the investor, see *supra* sub 4.1.

92 In the context of third-party effects of assignment, see Catherine Walsh, "The Role of Party Autonomy in Determining the Third-Party Effects of Assignments: Of 'Secret Laws' and 'Secret Liens'" (2018) 81 Law and Contemporary Problems 181, 190.

choice of law remains extremely rare in a space that is characterised by a general aversion to courts and the law. The question of whether the law governing proprietary issues regarding stablecoins could be chosen therefore remains, at least for the time being, largely theoretical.

4.2.7 Intermediate Conclusion

It does not seem promising to determine the applicable law with regard to proprietary effects on the basis of the *situs* of stablecoins. Instead, the focus should be on the administrator of the blockchain. In many cases, this might be the entity that issues stablecoins or that validates the assets that back up the stablecoin. However, it is not hard to imagine scenarios where different entities share powers and responsibilities; with more and more different business models, diversification might even increase. It is therefore crucial that PIL clearly defines which entity qualifies as issuer and validator. To avoid friction between regulatory provisions and civil law, the same entity that serves as connecting factor for PIL rules should, ideally, also be responsible for fulfilling regulatory duties. As always, the greater the consensus between the PIL legal systems of different states, the greater the synchronisation of the applicable laws.

4.3 *Law Applicable to the Assets Represented by the Stablecoin*

It is crucial to distinguish between the law applicable to the stablecoin, which has been discussed previously, from the law applicable to assets represented by the stablecoin. The determination of the latter depends on the kind of asset represented by the token. It is subject to the classic conflict-of-laws rules for property related issues.

4.3.1 *Lex Rei Sitae*

Where the stablecoin is backed by tangible assets, the law applicable to the latter is governed by the classic rule according to which the law at the location (*situs*) governs property matters. When stablecoins are linked to commodities like gold, the location of the physical asset therefore determines the law that applies to the question of ownership in that commodity. The *lex rei sitae* principle governs movable and immovable things alike. It also applies to other rights *in rem* regarding tangible property that may constitute the asset pool of a stablecoin, such as mortgages.

4.3.2 Law Governing Fiat Currency

Where the stablecoin represents a fiat currency, *e.g.* the US Dollar, the law applicable to this asset is the law of the issuing state. This follows from the

principle that the latter state has the authority to define the content of its currency via the *lex monetae*.[93] While the origins of this principle are in public international law, it also has repercussions on the conflicts level.

However, property rights in specific coins and bills will be governed by the rules applying to movables, i.e. the *lex rei sitae*. Customers of banks have no property rights on the money in their accounts, but merely claims. The law applicable to these claims typically is that of the bank; either by virtue of a choice of law or by virtue of the principle of the closest connection.

4.3.3 Law of the Intermediary

The assets in the stablecoin issuer's portfolio (asset pool) may be transferrable securities, such as shares or bonds. Typically, such securities are held with an intermediary (custodian). Depending on the applicable conflict rules of the deciding court, such securities may be governed by the law in force at the place of the custodian (so-called Place of the Relevant Intermediary Approach – PRIMA) or the law of the place where the account is administered by the latter (so-called *lex conto sitae*).[94]

4.3.4 *Lex Societatis*

The asset represented by a stablecoin may be a membership right in a company, for instance a share in a special vehicle that has no other purpose than to hold a certain portfolio of assets. If this is an uncertificated share – i.e., one that is not easily transferrable and cannot be traded, *e.g.* on an exchange –, there seems to be no room for the application of another law than the law governing the company to this share. Depending on the conflicts rule in force in the state of the deciding tribunal, this can be the law of the real seat or the law of the country in which the company has been incorporated (the *lex incorporationis*). If the share is certificated and not held with an intermediary, it will be subject to the *lex rei sitae* rule.

4.3.5 Law of the Claim

Where a stablecoin represents a claim, the question of whether this claim belongs to the asset pool and which rights the asset pool has with regard to third parties must be determined following the ordinary rules of PIL regarding the third-party effects of the assignment of claims. This is one of the most difficult areas of conflict of laws, and the solutions retained on the national level

93 See Charles Proctor, Mann on the Legal Aspect of Money (Oxford: OUP 2012), para 13.04.

94 See e.g. Matthias Lehmann, "Financial Instruments", in: Jürgen Basedow et al., Encyclopedia of Private International Law (Cheltenham: Edward Elgar 2017); André Ruzik, in: Matthias Lehmann and Christoph Kumpan (eds), European Financial Services Law (Baden-Baden: Nomos 2019), Art 9 FCD paras 9–10.

vary. An international convention concluded under the auspices of UNCITRAL suggests the application of the law of the assignor.[95] Switzerland, in contrast, follows the principle of party autonomy, and in the absence of a choice by the parties refers to the law governing the claim.[96] The European Union has yet to legislate on this issue, which has been spared by Art. 14 Rome I Regulation because of political differences between the Member States. The Commission has tabled a proposal which follows, in principle, the suggestion by UNCITRAL, but contains numerous exceptions.[97]

4.3.6 Law Governing Crypto Asset

A special case are stablecoins that refer to cryptocurrencies or other digital assets. With regard to the applicable law to them, there is still much legal uncertainty. Once consensus has been found regarding cryptocurrencies and other digital assets, these rules should also apply to them where they are used as assets backing up stablecoins.

4.3.7 Intermediate Conclusion

In sum, the traditional conflict-of-laws rules apply to proprietary questions regarding the assets of which a stablecoin portfolio is composed. It is neither theoretically nor practically sound to change existing PIL rules for assets outside the blockchain, as this would lead to legal uncertainty. Nor is such a change necessary, as established rules already exist. These rules cannot be overridden by other connecting factors merely because the assets are tokenised on a blockchain. This fact is often obfuscated by terms and whitepapers of stablecoin issuers who seem to suggest that tokenised assets would be outside any legal system.[98]

4.4 *Law Determining the Relationship between Token and Asset*

It follows from the above that the laws governing the stablecoin and the laws governing the assets represented by the stablecoin can diverge. Such cases of divergence will not be rare, but often a matter of course. To illustrate, it is clear

95 See United Nations, *UN Convention on the Assignment of Receivables in International Trade* (New York: UN Publications 2004), Art 30(1).

96 Swiss PILA (n 66), Art. 145.

97 European Commission, Proposal for a Regulation of the European Parliament and of the Council on the law applicable to the third-party effects of assignments of claims, [2018] COM/2018/096 final.

98 See for example the Paxos Whitepaper (Pax Gold, "White Paper" (*Paxos*, last updated 5 September 2019), 8 <https://paxos.com/wp-content/uploads/2019/09/PAX-Gold-White paper.pdf>): "Bitcoin enthusiasts are also often attracted to gold for many of their shared properties: they are decentralized, 'outside' assets that are no one else's liability and are not tied to any particular government […]".

that German law governs commodities that are situated in Germany and used as the underlying assets for stablecoins. Crucially, German law applies in this case independently of the law that governs the stablecoin. If the law of another state has been chosen to govern proprietary law questions regarding the stablecoin, or if the issuer of the stablecoin is incorporated outside of Germany, two different laws apply.

But there is an additional problem: which law determines the link between the commodities and the stablecoin? This link is decisive for important issues, such as whether the investors will have rights to access the underlying assets and how they will be protected in the case of insolvency of the intermediary.

The law governing this link must – logically – be distinguished from the law governing the stablecoin on the one hand and the law governing the asset represented by the stablecoin on the other. The need for the potential application of a third law is especially evident where the assets are held via an entity, such as a corporation, an association or a Digital Autonomous Organization (DAO). In these cases, it is particularly clear that the law governing the entity must be distinguished from the law governing the token or the asset. Yet even in the absence of such an entity, there is a need for identifying the law that links the asset with the stablecoin.

This means that, at least in an intermediate step, a third law enters the equation. The question of which law this should be and how it is to be determined is very important. The economic value of stablecoins – unlike cryptocurrencies such as Bitcoin – depends entirely on the link to the underlying asset. Without a firm relation between the stablecoin and the asset it represents, the former is essentially worthless and would hardly be accepted on the market.

However, the relationship between the stablecoin and the asset it represents is very tenuous. It is unclear which law should govern this relationship; the issue seems to fall between the cracks of the law governing the stablecoin and the law governing the asset represented by the stablecoin.

Again, the answer varies depending on the asset in question. For tangible assets represented by a stablecoin, it is undeniable that the *lex rei sitae* must have a determinative influence on the relation between this asset and the stablecoin. This is first because creditors, insolvency administrators, and other parties rightfully expect this law to govern the question of which assets are part of a stablecoin portfolio, for the simple reason that they cannot know whether these assets are part of such a portfolio in the first place. Secondly, the law where the assets are situated should be called upon to determine whether assets are represented by a stablecoin because this country exerts enforcement power over them.

To illustrate, a quantity of commodities that are to be represented by a stablecoin may be situated in country X, while the stablecoin itself may be governed by the law of country Y as the chosen law for the token. It would make little sense to extend the choice of law that has been made for the stablecoin to the

commodities it represents. The latter, as tangible assets, are governed by the law of their location, which determines the property rights in them. Whether these property rights can be transferred via the blockchain must be determined by the law governing the commodities as well because the blockchain cannot withdraw assets from the scope of the *lex rei sitae* without the latter's permission.

This rather clear case should not lead to the conclusion that the law governing the asset would always rule over the possibility of including the asset into a stablecoin portfolio and transferring it with the transfer of the stablecoin. A counterexample can be found in Article 145a Swiss PILA. This provision sets out the law governing the question whether a claim is represented by a negotiable instrument in paper "or in equivalent form". This last formula has been added to accomodate new phenomena related to DLT.[99] Article 145a Swiss PILA thus concerns exactly the problem discussed here, i.e. the identification of the third law that links the asset, in this case claims, to the token. It does so in a peculiar way: In the first place, the provision refers to the law identified in the negotiable instrument itself, thereby giving room to the principle of party autonomy. In the absence of a choice of law in the instrument, Article 145a Swiss PILA calls upon the law of the seat of the issuer or its habitual residence. This latter connecting factor does not necessarily result in the same law as that governing either the instrument – the token – or the asset represented by it – the claim. Rather, it can lead to the application of a third law. The idea behind this rule was to better protect third parties that may be unaware of the law governing the underlying claim.[100] It also chimes with the general rules applying to the third party effects of assignment under the UN Convention on the Assignment of Receivables and the EU Proposal of 2018 on the subject.[101]

Though the Swiss solution is – at least for the moment – pretty singular, with other jurisdictions not having even started to deal with the problem it proves the point made here: the legal system governing the linkage and the law(s) governing the token and the asset may differ.

In sum, the law determining whether an asset is part of a stablecoin portfolio must be distinguished from the law governing the stablecoin on the one hand and the assets of the portfolio on the other. While all three laws may fall into one, this is not necessarily always the case. For instance, the law governing

99 See the introduction by the Act for the adaption of Federal Law to the Development of Distributed Electronic Registers, Swiss Federal Gazette 2020, p. 7801, 7807. On the rationale of the provision, see Swiss Federal Council (n 32), p. 299-300.

100 See Swiss Federal Council id.; Andrea Bonomi in Bernard Dutoit and Andrea Bonomi (eds), Droit international privé suisse - Commentaire de la loi fédérale du 18 décembre 1987, 6th ed. (Basel: Helbing Lichtenhahn 2022), Art 145a para 8.

101 UN Convention on the Assignment of Receivables, done on 12 December 2001 in New York, Art 30(1); EU Commission (n 98) Art 4(1).

claims may diverge from the law that decides whether they form part of a stablecoin portfolio, while the coin itself may be subject to a third law.

5 Conclusion

One needs to distinguish between tokens, assets, and the relation between the token and the underlying asset. PIL should consider this differentiation and provide for potentially three different connecting factors. As a consequence, there may be three different laws that apply: the law governing the stablecoin itself, the law governing the asset represented by the stablecoin, and the law governing the relation between the stablecoin and the asset represented. While they may sometimes be identical, this is not universally the case. To make the stablecoin arrangement effective and protect the interests of the investors, some coordination between those legal systems is needed.

For the relation between the stablecoin issuer and the investor, choice of law by the participants should be allowed subject to typical restrictions, in particular consumer protection provisions. For the stablecoin itself, the location of the issuer of the coin or of the validator of the portfolio may be used as a connecting factor. The law applicable to assets represented by a stablecoin must follow existing PIL rules. In particular, the property aspects of corporeal assets should not be treated differently just because they are tokenised on a blockchain.

Most importantly, clear rules are needed to define the relationship between the tokens and the linked assets. The differences between the PIL rules in addition to diverging substantive law rules in this regard pose a significant obstacle for stablecoin business models. A solution could be substantive law harmonisation. However, as this will always remain incomplete, one must also harmonise the rules of PIL. The most sensible place for new PIL rules would be an international convention. It should contain general rules on the determination of the law governing cryptocurrencies and tokens. As for stablecoins, its most significant contribution would be to identify the law that governs the link between the stablecoin itself and the assets backing it.

CHAPTER 14

The Tort Law Applicable to the Protection of Crypto Assets

Tobias Lutzi

1 Introduction

As the different contributions to this book aptly demonstrate, Private International Law (PIL) often struggles to accommodate phenomena that lack a sufficiently substantial connection to the territory of a particular legal system. The protection of crypto assets against tortious interference in the form of theft, manipulation, fraud, or extortion is no exception.

This difficulty is, for at least three reasons, especially pronounced in the area of tort law.[1] First, the parties are generally not bound by any pre-existing relationship that might help to identify the law that is most closely connected. Second, PIL traditionally reacts to such a lack of meaningful connections other than the tort itself by relying on purely geographical connecting factors such as, most importantly, the "place" of the tort – which is inherently difficult to identify in the context of digital assets. Third, some of the core features of many crypto assets – such as the decentralised nature of the underlying networks and the pseudonymity of their users[2] – further complicate the application of traditional conflicts rules.[3]

This is not to say that PIL is unable to identify the applicable tort law to the protection of crypto assets.[4] While a variety of situations potentially fall into this category (2.), the traditional conflicts rules for torts accommodate them

1 This may also be the reason why the topic has so far received far less attention than the question of the applicable contract law.

2 As is regularly pointed out, the offline identity of Bitcoin inventor(s) Satoshi Nakamoto remains unknown to this day.

3 See also Andrew Dickinson, "Cryptocurrencies and the Conflict of Laws," in David Fox and Sarah Green (eds), *Cryptocurrencies in Public and Private Law* (Oxford: Oxford University Press 2019), para. 5.08; Matthias Lehmann, "Internationales Privat- und Zivilprozessrecht," in Sebastian Omlor and Mathias Link (eds), *Kryptowährungen und Token* (Frankfurt am Main: dfv 2021), paras. 22–26.

4 For a similar conclusion, see Matthias Lehmann, "Who Owns Bitcoin? Private Law Facing the Blockchain" (2019) 21 Minnesota Journal of Law, Science & Technology 93, 132–33.

© TOBIAS LUTZI, 2023 | DOI:10.1163/9789004514850_016
This is an open access chapter distributed under the terms of the CC BY-NC-ND 4.0 license.

with difficulty and to vastly different degrees. Thus, the *lex loci delicti* rule can be applied with somewhat surprising ease if it is understood to refer to the place of the relevant act(s) but struggles in its (now more common) understanding as the place of the damage (3.). In many cases, this difficulty can, however, be overcome by more flexible provisions that refer more broadly to the law most closely connected to the case at hand (4.). Rules for specific torts (5.) and party autonomy (6.) may also play a residual role, while proposals to simply sidestep the conflict-of-laws analysis by applying the so-called *lex cryptographica* must ultimately be rejected (7.). Perusing the rich toolbox of PIL in view of the specific challenge of protecting crypto assets in tort law thus reveals a number of strengths and weaknesses that we also observe in other cases of online torts (8.).

2 The Protection of Crypto Assets and Tort Law

Before discussing the application of specific conflicts rules to the protection of crypto assets, it might be helpful to specify which cases fall into this category (2.1). The extent to which these cases actually are subject to the conflicts rules on torts is, of course, a question of characterisation, the answer to which may differ depending on the relevant legal system (2.2).

2.1 *The Protection of Crypto Assets*

The protection of crypto assets against tortious interference and misappropriation may refer to a wide range of different situations, not all of which necessarily create novel challenges for existing conflicts rules. In order to structure the discussion of their application in the following sections, it appears useful to sort them into two separate sets of problems.

The first set involves interference with crypto assets held by another individual. Control over these assets is usually exercised through a set of keys stored in a wallet held either by the "owner" or by some intermediary (*e.g.* a centralised crypto exchange).[5] These keys may be stolen, intentionally deleted or destroyed, or simply lost.[6] Their owners may also be tricked or coerced into using them to transfer their assets to someone else.

5 Examples include *Bisq*, *Binance*, *Coinbase* and *Kraken*.

6 It is believed that about 20% of all bitcoins are lost forever because their owners have simply misplaced or permanently deleted their private keys; as of August 2021, the value of these lost coins would amount to more than 140 billion Euros.

If the assets in question involve a physical device (*e.g.* a hard disk or USB flash drive), this may simply be stolen or destroyed, which would hardly raise any new questions of PIL.[7] The fact that the stolen device contains data that gives access to assets stored on a blockchain should not distract from the fact that all relevant aspects of the tort can be localised by looking purely at its physical elements. Much like the tort law applicable to the theft of a car does not change depending on what was stored in the trunk, the law applicable to the theft of computer hardware should not depend on what was stored on it. Other types of interference with someone else's hardware, including its temporary deactivation or permanent destruction, should similarly be treated independently of whether or not the hardware was used to access crypto assets.[8]

On the other hand, where the interference is independent of where the key is stored physically, for example because it is accessed by the tortfeasor remotely or because the owner is tricked or coerced into acquiring or transferring certain assets, identifying the applicable law becomes more complicated. Considering the continuing popularity of cryptocurrencies for all kinds of cybercrimes[9] as well as the rapidly growing importance of NFTs, this scenario is arguably the most practically relevant, as a growing number of reported cases illustrates. In three cases recently decided by the Commercial Court of the High Court of Justice of England and Wales,[10] the claimants alleged that they were coerced into transferring US$ 950,000 worth of bitcoin as a ransom;[11] that they transferred £577,000 worth of bitcoin in the context of an initial coin offering fraud;[12] and that they lost US$ 2.6m as a result of crypto assets being transferred by hackers accessing their crypto wallet.[13] In the District Court for the Central District of California's recent decision in *Terpin v. AT&T Mobility*,[14] hackers had allegedly gained control over the claimant's mobile phone number

7 See also Dickinson (n 3), para. 5.11.

8 *Id.*

9 The latest Cryptocurrency Crime and Anti-Money Laundering Report by CipherTrace puts the overall volume of "crypto crime" at $1.9 bn, the vast majority of which consists of fraud and misappropriation: see CipherTrace, "Cryptocurrency Crime and Anti-Money Laundering Report" (*CiperTrace*, February 2021), 6–7 <https://ciphertrace.com/wp-content/uploads/2021/01/CipherTrace-Cryptocurrency-Crime-and-Anti-Money-Laundering-Report-012821.pdf> accessed 1 June 2022.

10 As to which see also Amy Held, Chapter 8 of this volume, subs. 2.3 and 2.4.

11 *AA v. Persons Unknown et al.*, [2019] EWHC 3556 (Comm).

12 *Ion Science Ltd v Persons Unknown & Others*, EWHC (Comm), 21 Dec 2020, reported by Amy Held, "Does situs actually matter when ownership to bitcoin is in dispute?" (2021) 36 Journal of International Banking and Financial 269, 269–272.

13 *Fetch.AI Limited et al. v. Persons Unknown et al.* [2021] EWHC 2254 (Comm).

14 *Terpin v. AT&T Mobility*, 2019 WL 3254218 (C.D. Cal. 2019).

on two occasions in order to impersonate him and gain access to his crypto wallet, ultimately stealing tens of millions of dollars' worth of cryptocurrency. While it might still be possible to localise certain elements of the tort in these cases, identifying the place of the damage can easily become very difficult.[15]

A second set of problems involves interferences with the crypto network itself. The degree of complexity and organisation of the different networks varies as widely as their vulnerability to cyber-attacks. In another Californian case, *Fabian v. LeMahieu*,[16] for instance, the plaintiff claimed he lost substantial amounts of cryptocurrency as part of a series of unauthorised transactions on the defendant's cryptocurrency exchange that resulted in a loss of assets worth US$ 170 million in total. Similarly, the DAO, arguably the most famous example of a decentralised autonomous organisation, became subject to an exploit that allowed one or several users to misappropriate about a third of its funds (which exceeded US$ 100 million at the time).[17] In reaction to the attack, the Ethereum blockchain was reset to before the attack, creating a permanent fork in the process.[18] The highly decentralised control of many blockchains also allows for subtler ways of manipulation. As many blockchains rely on consensus mechanisms, they can be manipulated (within limits) by anyone who manages to control a sufficiently high number of nodes (so-called "51 percent attacks").

As explained in the following sections, this latter group of torts – *i.e.* those directly targeting the crypto network – are the most difficult for PIL to accommodate. PIL struggles with both delocalised torts and torts involving more than two parties.[19]

2.2 *The Scope of the Applicable Tort Law*

Although each legal system is free to decide which cases it characterises as torts for the purpose of the conflict of laws, a number of general observations can be made in the present context.

First, all the situations described above necessarily involve a crypto network that operates according to certain rules, which may give rise to legal relationships that can be characterised as contractual (or even corporate).[20] Of course, this does not mean that all the claims described previously will follow this

15 See *infra* section 3.2.

16 *Fabian v. LeMahieu*, 2019 WL 4918431 (N.D. Cal. 2019).

17 See also Florence Guillaume and Sven Riva, Chapter 20 of this volume, sub. 2.1.

18 Called Ethereum Classic.

19 See also Dickinson (n 3), para. 5.12.

20 *Id.*, paras. 5.27–34.

characterisation. As explained above, if a physical device is stolen, the fact that the assets stored on it derive their value from the existence of a decentralised global network of contractual relationships will not change the characterisation of its owner's claim in tort. Yet, the more closely the facts of the case are connected to this network, the more difficult it will be to draw the line between contract and tort.

As far as EU instruments of PIL[21] are concerned, the (slightly wider) category of non-contractual obligations is traditionally defined by reference to contractual obligations,[22] *i.e.* obligations "freely assumed by one party towards the other."[23] But even where the parties are bound by a contract in this sense, not all claims between them will automatically fall under the conflicts rules for contracts. According to the latest iteration of the relevant formula stated by the Court of Justice of the European Union (CJEU), a claim will still be characterised as non-contractual "where the applicant relies, in its application, on rules of liability in tort, delict or quasi-delict, namely breach of an obligation imposed by law, and where it does not appear indispensable to examine the content of the contract concluded with the defendant in order to assess whether the conduct of which the latter is accused is lawful or unlawful."[24]

While other legal systems may have found more elegant ways to draw the line (or not to require such line drawing), it seems fair to say that except for violations of a crypto network's rules by one of its participants that directly affect other participants, the situations described above will give rise to claims that can safely be characterised as non-contractual. This is true for cases of theft or misappropriation of crypto assets, fraudulent misrepresentation and prospectus liability[25] as well as for external attacks on the functioning of the crypto

---

21 In particular, Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), [2008] OJ L177/6 ("Rome I Regulation") and Regulation No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II), [2007] OJ L 199/40 ("Rome II Regulation").

22 See Judgment of the Court (Fifth Chamber) of 27 September 1988, *Athanasios Kalfelis v Bankhaus Schröder, Münchmeyer, Hengst and Co. et al.*, Case 189/87 (ECLI:EU:C:1988:459), paras. 17–18.

23 See Judgment of the Court of 17 June 1992, *Jakob Handte & Co. GmbH v Traitements Mécano-chimiques des Surfaces SA*, ECR I-03967, Case C-26/91 (ECLI:EU:C:1992:268), para. 15. On the need for a consistent interpretation of the different instruments, see Recital (7) of both the Rome I (n 21) and Rome II (n 21) Regulations.

24 Judgment of the Court (Grand Chamber) of 24 November 2020, *Wikingerhof GmbH & Co. KG v Booking.com BV*, Case 59/19 (ECLI:EU:C:2020:950), para. 33.

25 Judgment of the Court (Fourth Chamber) of 28 January 2015, *Harald Kolassa v Barclays Bank plc*, Case C-375/13 (ECLI:EU:C:2015:37), paras. 36–41. See also Landgericht Berlin,

network or ledger technology. Yet, as discussed below, this characterisation does not necessarily prevent taking into account the contractual relationship.[26]

Second, not all situations involving non-contractual obligations are necessarily governed by the general conflicts rules on torts. On the one hand, some might escape these rules altogether as a consequence of being subject to more specific instruments such as the EU General Data Protection Regulation.[27] The Rome II Regulation also carves out an exception for negotiable instruments in its Article 1(2)(c), albeit with a limited scope that does not appear to extend to crypto assets.[28] On the other hand, specialised rules may apply to particular torts involving crypto assets, such as product liability,[29] unfair competition,[30] and infringement of IP rights.[31]

Third, a number of questions that appear to safely fall outside the ambit of tort law can arise as preliminary questions to a claim in tort. This might be particularly relevant for the question of ownership.[32] While many legal systems resolve these questions by applying the relevant conflicts rule of the *lex fori* independently of the law applicable to the main question, others subject both questions to the latter.[33]

Fourth, questions that fall under the applicable substantive (tort) law must also be distinguished from questions of procedure, which are traditionally

---

Case 2 O 322/18, 27 May 2005, ECLI:DE:LGBE:2020:0527.20322.18.00, para. 109, for a case of prospectus liability in the context of an Initial Coin Offering (ICO).

26 See *infra* section 4.

27 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L119/1 ("GDPR").

28 See Björn Steinrötter, "International Jurisdiction and Applicable Law," in Philipp Maume, Lena Maute, and Mathias Fromberger (eds), *The Law of Crypto Assets. A Handbook* (Munich/Oxford/Baden-Baden: Beck/Hart/Nomos 2022), para. 45; Dieter Martiny, "Virtuelle Währungen, insbesondere Bitcoins, im Internationalen Privat- und Zivilverfahrensrecht" (2018) 38 Praxis des Internationalen Privat- und Verfahrensrechts 553, 560, 564.

29 See, *e.g.*, Article 5 of the Rome II Regulation (n 21).

30 See, *e.g.*, *id.*, Article 6.

31 See, *e.g.*, *id.*, Article 8. See also the rules on *culpa in contrahedo* (*id.*, Article 12; which are particularly relevant in cases of fraud) and unjust enrichment (*id.*, Article 10).

32 See also Susanne Lilian Gössl, "IPR und Smart Contracts," in Thorsten Voß (ed), *Recht der FinTechs – Legal Aspects of Financial Technology* (Berlin: De Gruyter 2021), para. 79; Matthias Lehmann, "Internationales Finanzmarktrecht," in Jan von Hein (ed), *Münchener Kommentar zum Bürgerlichen Gesetzbuch* (8th edn, München: Beck 2021), vol. 13, part 12, para. 603.

33 See Andrea Bonomi, "Incidental (preliminary) question," in Jürgen Basedow et al. (eds), *Encyclopedia of Private International Law* (Cheltenham/Northhampton: Edward Elgar 2017), 913–14.

governed by the *lex fori*.[34] Thus, while the applicable tort law may determine which remedies are available,[35] it will ultimately depend on the *lex fori* if a court will be able to award damages in a cryptocurrency.[36]

3 The Place of the Tort

Over the last few centuries, the *lex loci delicti commissi* rule has clearly emerged as the principal conflict-of-laws rule in the area of tort law.[37] It provides the starting point, in some form or another, in the vast majority of PIL systems.[38] Its significance is based on its generally strong connection to the tort in question (especially where the parties had no other prior contacts), its predictability for both parties, and its perceived neutrality.[39] As the number of torts "happening" in more than one "place" grew rapidly during the 20th century, though, a choice between the place of the relevant act(s) and the place where these acts produced their harmful effect(s) became necessary.[40] While many legal systems have opted for one or the other,[41] some legal systems leave the choice to the claimant.[42]

---

34 See Paul Torremans et al. (eds), *Cheshire, North & Fawcett. Private International Law* (Oxford: Oxford University Press 2017), 73: "One of the eternal truths of every system of private international law is that a distinction must be made between substance and procedure, between right and remedy. The substantive rights of the parties to an action may be governed by a foreign law, but all matters appertaining to procedure are governed exclusively by the law of the forum."

35 See Article 15(c) of the Rome II Regulation (n 21).

36 See Dickinson (n 3), paras. 5.89–92 (on English law).

37 See Thomas Kadner Graziano, "Torts," in Jürgen Basedow et al. (eds), *Encyclopedia of Private International Law* (Cheltenham/Northhampton: Edward Elgar 2017), 1709, 1710; Stig Strömholm, "Intentional Torts," in Kurt Lipstein (ed), *International Encyclopedia of Comparative Law. Vol. III: Private International Law* (Tübingen/Leiden/Boston: Mohr Siebeck/Martinus Nijhoff 1980), ch. 33, para. 1.

38 Graziano (n 37), 1710–11.

39 *Id.*, 1711.

40 *Id.*, 1714.

41 *E.g.,* Article 4(1) of the Rome II Regulation (n 21) (place of the damage); Article 133(2) of the Swiss PILA (Federal Act on Private International Law (PILA) of 18 December 1987, SR 291) (place of the damage); Article 8(2) of the Rome II Regulation (n 21) (place of the causal event).

42 *E.g.*, Article 40(1), 2nd sentence, of the German Introductory Act to the Civil Code ("EGBGB") (Einführungsgesetz zum Bürgerlichen Gesetzbuche in der Fassung der Bekanntmachung vom 21. September 1994 (BGBL. I S. 2494; 1997 I S. 1061), das zuletzt durch Artikel 3 des Gesetzes vom 21. Dezember 2021 (BGBL. I S. 5252) geändert worden ist).

The following section will discuss how each of these two places could be identified with regard to the protection of crypto assets.

3.1 *The Place of the Relevant Act*

The connecting factor of the place of the relevant act (*locus actus*; causal event) does not raise insurmountable difficulties when applied to torts involving crypto assets.[43]

For torts involving physical acts, the involvement of crypto assets evidently raises no particular problems in this regard: as far as conflict-of-laws rules are concerned, there is no reason to treat the theft of a USB drive that contains a crypto wallet and the theft of a physical wallet that contains bank notes differently. However, even for torts that lack a physical interaction between the parties, such as the theft of crypto assets through hacking, the criterion of the place of the causal event remains helpful as even those torts will usually involve an action or decision that can be pinpointed to a specific place. It is this versatility of the criterion that has led Peter Mankowski to describe the *locas actus* as a "sleeping beauty" (in the context of international jurisdiction).[44] Besides, the criterion also has the advantage of best reflecting the defendant's expectations as to the legal system governing its behaviour, even where it takes place online.[45]

The criterion however runs into problems when applied to torts that consist of multiple acts that do not necessarily take place in a single country. Where these acts are committed by different alleged tortfeasors (*e.g.* in a Distributed Denial of Service (DDoS) attack), the law of each place of acting can easily be applied to each of them. Where these acts are committed by a single tortfeasor, on the other hand, it appears appropriate to try to identify the most significant act, the location of which should determine the applicable law. This would be in line with the jurisprudence of the CJEU, which has held that even in case of consecutive acts of infringement of a Community Design,

> the correct approach for identifying the event giving rise to the damage [under Article 8(2) of the Rome II Regulation] is not to refer to each alleged act of infringement, but to make an overall assessment of that

43 See also Martiny (n 28), 564; Tobias Lutzi, *Private International Law Online* (Oxford: Oxford University Press 2020), para. 5.79 (regarding its appropriateness in internet cases more generally).

44 Peter Mankowski, "Der Deliktsgerichtsstand am Handlungsort – die unterschätzte Option," in Rolf A. Schütze (ed), *Fairness Justice Equity. Festschrift für Reinhold Geimer zum 80. Geburtstag* (Munich: Beck 2017), 430.

45 Lutzi (n 43).

> defendant's conduct in order to determine the place where the initial act of infringement at the origin of that conduct was committed or threatened.[46]

Although identifying this place may not always be straightforward in purely practical terms,[47] if the claimant has already managed to identify an alleged tortfeasor, the claimant might also be able to pinpoint a place in which the defendant may plausibly have acted.[48]

In the context of trademark infringements committed by reserving certain key words in Google's AdWords service,[49] the CJEU has also decided that the relevant act[50] is the activation of a technical process, rather than its execution by a service provider.[51] This reasoning can helpfully be extended to the use of bots and algorithms.

Where it is impossible to identify a particularly relevant act out of numerous acts spread across different countries, a sensible fallback option might consist in applying the law of the alleged tortfeasor's country of habitual residence, at least if it is among the countries in which the alleged tortfeasor has acted.[52] This might also provide a solution for cases that would otherwise produce completely arbitrary results (*e.g.* where a tort is committed while travelling on a train that passes numerous countries) or would be open to manipulation – if

---

46 Judgment of the Court (Second Chamber) of 27 September 2017, *Nintendo Co. Ltd. v BigBen Interactive GmbH and BigBen Interactive SA*, Joined Cases C 24/16 and C 25/16 (ECLI:EU:C:2017:724), para. 103. See also Judgment of the Court (Fourth Chamber) of 21 May 2015, *Cartel Damage Claims (CDC) Hydrogen Peroxide SA v Akzo Nobel NV et al.*, Case C-352/13 (ECLI:EU:C:2015:335), paras. 47–49, for some similar considerations regarding international jurisdiction.

47 See Florence Guillaume, "Aspects of private international law related to blockchain transactions," in Daniel Kraus, Thierry Obrist, and Olivier Hari (eds), *Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law* (Cheltenham: Edward Elgar 2019), 64.

48 See also Dickinson (n 3), para. 5.12.

49 Rebranded as Google Ads in 2018.

50 For the purpose of jurisdiction under Article 7(2) of the Brussels Ia Regulation (Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, [2012] OJ 351/1) ("Brussels Ia Regulation").

51 Judgment of the Court (First Chamber), 19 April 2012, *Wintersteiger AG v Products 4U Sondermaschinenbau GmbH*, Case C523/10 (ECLI:EU:C:2012:220), para. 34. See also Judgment of the Court (Fourth Chamber) of 22 January 2015, *Pez Hejduk v EnergieAgentur. NRW GmbH*, Case C-441/13 (ECLI:EU:C:2015:28), para. 24.

52 See Mankowski (n 44), 435.

the legal system in question does not allow for exceptions to the strict *lex loci delicti* approach anyway.[53]

3.2 *The Place of the Damage*

Although often lauded for its higher degree of predictability,[54] the place of the damage (*locus damni*) is a notoriously problematic connecting factor for online torts,[55] which often produce effects in many places at once while having virtually no connection to any particular physical place.[56] As far as crypto assets are concerned, these problems manifest themselves in both types of situations described above.

Regarding tortious interference with someone else's assets, the difficulty will usually consist in identifying the place where the damage materialised. Except for cases of theft or destruction of a physical device containing a private key, the immediate damage will usually consist in nothing more than a certain asset no longer being linked to the victim's public key. This is true for a wide range of torts, from the theft of a private key through hacking (and subsequent transfer of funds) to the extortion of crypto assets. In all of these cases, identifying the *lex loci damni* will make it necessary to localise the loss of the asset. This can arguably be done in two ways. First, the loss could be understood as being the consequence of a specific block being irreversibly added to the ledger in question, making every place in which the latter is physically stored a place of the damage. For a technology that relies on the widespread, potentially global distribution of the relevant information, this hardly seems helpful. Second, the loss could be understood to occur in the place in which the victim's wallet is stored. While this might instinctively appear as a more appropriate solution, it will rarely constitute an actual improvement over the former approach: since a wallet ultimately consists of nothing more than a set of keys, which can be stored on countless different media and in an infinite number of places, the location of the wallet is almost as unpredictable and arbitrary as the location of the ledger.[57]

Still, focusing on the wallet reveals another, potentially more helpful avenue. Given that control over a wallet is exercised through mere knowledge of a unique combination of letters and numbers, it might be considered to be

53 See *infra* section 4.

54 See Proposal for a Regulation of the European Parliament and the Council on the Law Applicable to Non-Contractual Obligations ("Rome II"), COM(2003) 427 final, 2003/0168 (COD), 11–12.

55 See Lutzi (n 43), para. 4.68.

56 Lutzi (n 43), paras. 2.35–40.

57 See also Guillaume (n 47), 63–64; Steinrötter (n 28), para. 48.

located wherever the person, who either has legitimate knowledge of the key or effectively controls the access to it, is located. Accordingly, the wallet could be considered to be localised either at the seat of the entity controlling the wallet on behalf of its "owner"[58] or at the habitual residence of said "owner."[59] The High Court of Justice of England and Wales seems to have adopted a similar approach when it considered English law to apply to alleged torts against victims domiciled in England.[60] These decisions have been criticised for equating the "owner's" domicile with the *situs* of the cryptocurrencies controlled by them[61] and for failing to take into account the case law of the CJEU,[62] which is indeed notoriously hesitant to equate the place in which the claimant's assets are concentrated with the place of damage in cases of pure financial loss.[63] Still, the particular importance of effective control in the context of crypto assets indeed provides a powerful argument in favour of considering the place from which such control is exercised as the place in which the relevant loss occurred.

If the victim does not transfer crypto assets, but is tricked into paying traditional currency in exchange for crypto assets that later turn out to be worthless, the immediate damage could plausibly be considered to already materialise in the victim's bank account, rather than in the crypto wallet. In a series of decisions on cases of prospectus liability (which is not free from ambiguity),[64] the CJEU has indicated that at least where the assets acquired have effectively

58 See Gössl (n 32), para. 73.

59 For similar lines of reasoning, see Dickinson (n 3), para. 5.12; Lehmann (n 32), para. 605; Lehmann (n 3), paras. 213–14; Martiny (n 28), 564. *Contra* Guillaume (n 47), 65.

60 *Fetch.AI Limited et al.* (n 13), para. 14; *Ion Science Ltd* (n 12), reported by Held (n 12). See also, in more detail, Held, Chapter 8 of this volume, sub 2.3 and 2.4.

61 See Held (n 12), 272.

62 See Amy Held and Matthias Lehmann, "Hacked crypto-accounts, the English tort of breach of confidence and localising financial loss under Rome II" (2021) 36 Journal of International Banking and Financial Law 708, 710–11; Amy Held and Matthias Lehmann, "Hacked Crypto-Accounts and the Continued Importance of Rome II in the English Courts: Fetch.AI v Persons Unknown" (*The EAPIL Blog*, 18 January 2022) <https://eapil.org/2022/01/18/hacked-crypto-accounts-and-the-continued-importance-of-rome-ii-in-the-english-courts-fetch-ai-v-persons-unknown/>.

63 See Judgment of the Court (Second Chamber) of 16 June 2016, *Universal Music International Holding BV v Michael Tétreault Schilling and Others*, Case C-12/15 (ECLI:EU:C:2016:449), paras. 31–32, 35; Judgment of the Court (Second Chamber) of 10 June 2004, *Rudolf Kronhofer v Marianne Maier and Others*, Case C-168/02 (ECLI:EU:C:2004:364), para. 20. See also Matthias Lehmann, "Where Does Economic Loss Occur?" (2011) 7 Journal of Private International Law 527, 537–540.

64 See Tobias Lutzi, "Ein wenig Wind um nichts: Das Bankkonto als Schadensort?" (2019) 39 Praxis des Internationalen Privat- und Verfahrensrechts 290, 290 et seq.

been worthless at the time of purchase, the place of the immediate damage is the place of the victim's bank account (*i.e.* the seat of the bank).[65]

Finally, if a tort is directed at the crypto network itself, for example because it is committed through manipulation of the consensus mechanism, there seems to be no way around trying to localise the ledger itself. Since it is a feature of most DLT applications that the ledger is simultaneously stored in a high number of virtually unpredictable places, this exercise will often result in a vast mosaic of applicable laws.[66] In closed and relatively small networks, which can be administered by even a single entity, it might indeed be possible to pinpoint the 'location' of the network. In all other cases, though, the *locus damni* should ideally provide nothing more than a starting point for the search of the law most closely connected to the case.

4 The Closest Connection

One of the reasons that the *lex loci delicti commissi* rule has stood the test of time despite the inappropriate results it occasionally produces is the fact that many legal systems allow their courts to deviate from its mechanical application in appropriate cases. While this deviation originally concerned cases in which both parties had a common domicile or residence in a country other than the one of the tort,[67] some systems, including the Rome II Regulation[68] (the provisions of which will continue to apply in the UK),[69] have meanwhile adopted a more open-textured exception that allows for the application of the law of the country to which the case is "manifestly more closely connected."[70]

Such escape clauses are particularly useful in the growing number of situations that only have a tenuous connection to the *locus delicti* (if at all), but may still be connected to a particular legal system. This is the case for many torts

65 Judgment of the Court (First Chamber) of 12 September 2018, *Helga Löber v Barclays Bank PLC*, Case C-304/17 (ECLI:EU:C:2018:701), para. 36; *Harald Kolassa* (n 25).

66 See Lehmann (n 3), paras. 207–08. Applying these laws distributively (following the so-called "mosaic approach") is only possible where the resulting damage can be split between the different countries concerned.

67 Graziano (n 37), 1711. See also Article 4(2) of the Rome II Regulation (n 21); Article 133(1) of the Swiss PILA (n 41).

68 Article 4(3) of the Rome II Regulation (n 21).

69 By virtue of Section 3 of the UK European Union (Withdrawal) Act 2018 and the Law Applicable to Contractual Obligations and Non-Contractual Obligations (Amendment etc) (EU Exit) Regulations 2019, SI 2019/834, as amended by SI 2020/1574, Regulation 11.

70 On the underlying rationale, see COM(2003) 427 final, 2003/0168 (COD) (n 54), 12–13.

that are committed online, which increasingly take place within the normative environments of online platforms and similar ecosystems.[71] Similarly, while a tort the measurable effects of which are limited to a distributed ledger can prove difficult or even impossible to localise, it may still be closely connected to a particular legal system.[72]

Applying the escape clause to such a tort makes it possible, first, to take a pre-existing relationship between the parties into account.[73] Where the parties are personally bound to each other by a contract, the escape clause enables the courts to apply the *lex contractus* to all related claims between these parties. In the present context, this is especially relevant for active participants (nodes) in the same network, whose relationship may be characterised as contractual (depending on the nature and rules of the network in question).[74] While identifying the *lex contractus* will still be difficult even in this type of situation, the aim of legal certainty strongly militates in favour of extending the result of this exercise to any parallel claim in tort.

Even where the parties are not bound by a contract *inter se*, they may still be connected through a network of contracts that establishes a close link to a particular legal system. Especially in closed, centrally administered blockchains, participants will regularly be in a relationship with the host or administrator that can fairly be characterised as contractual. If these individual contracts contain a choice-of-law clause,[75] it should very much be in the interest of legal certainty to extend this choice also to the relationships between participants.[76] The same might be true for open networks that require all participants to agree to certain terms and conditions pointing expressly or implicitly to a certain legal system,[77] or if tokens are acquired under a law chosen by the parties to the transactions and the alleged tortfeasor (who may even by one of these parties)[78] is aware of this choice. If no choice has been made, it might still be possible to identify a close connection to a legal system, which would be

71 See Lutzi (n 43), paras. 5.122–24.

72 See also Michael Ng, "Choice of law for property issues regarding Bitcoin under English law" (2019) 15 Journal of Private International Law 315, 336–38 (regarding questions of property); Steinrötter (n 28), para. 49; Gössl (n 32), para. 74.

73 See Article 4(3), 2nd sentence, of the Rome II Regulation (n 21): "A manifestly closer connection with another country might be based in particular on a pre-existing relationship between the parties, such as a contract, that is closely connected with the tort/delict in question." See also Article 133(3) of the Swiss PILA (n 41). See also Martiny (n 28), 564.

74 See Dickinson (n 3), paras. 5.27–34.

75 Which is not unusual: see Lehmann (n 3), para. 150.

76 See Gössl (n 32), para. 75. See also Lutzi (n 43), para. 5.144, by analogy.

77 See Ng (n 72), 338 (regarding Bitcoin).

78 See Landgericht Berlin (n 25), para. 116, for a case of prospectus liability.

justified not only by considerations of party expectations and legal certainty but also by policy considerations: as more and more states are starting to claim prescriptive jurisdiction over (certain) crypto networks, it appears sensible to align the applicable tort law with the legal system to which a particular network is particularly closely connected.

A number of factual elements can be considered in order to establish such a relevant connection:[79] the nature of the right for tokens that transfer a right;[80] the seat of the administrator for centrally administered ("permissioned") ledgers;[81] the expectations of the initial programmers of the algorithm as to the governing law, as far as it is identifiable (sometimes referred to as the *lex creationis*);[82] the seat of the supervisory authority, as far as it can be identified with reasonable certainty.[83] Formulating general rules as to which of these connecting factors should take precedence would not only far exceed the scope of this paper but also hardly be possible given the wide range of torts and crypto networks, and their rapidly evolving structure. Still, if several of the aforementioned factors point towards the same legal system, the case for displacing the traditional *lex loci delicti* approach becomes increasingly convincing.[84]

5 Rules for Specific Torts

In reaction to the growing importance of tort law and the increasingly wide range of torts governed by the same set of general connecting factors, many systems have adopted specialised rules to cover specific types of torts for which the *lex loci delicti* rule has proven particularly inadequate.[85] In the present context, these rules should only play a residual role. Where they apply, though, the fact that they often focus on particular elements of the tort that are usually both more appropriate and easier to identify than the *locus delicti* significantly facilitates the conflicts analysis in cases of torts against virtual assets.

79 See also Gössl (n 32), para. 74.

80 See Landgericht Berlin (n 25), para. 115; see also Lehmann (n 3), paras. 172–174.

81 See Lehmann (n 3), paras. 157–158; Lehmann (n 32), para. 605.

82 See also Lehmann (n 3), paras. 151–154.

83 See *id.*, paras. 155–156; Gössl (n 32), para. 74; Steinrötter (n 28), para. 49–50.

84 See Landgericht Berlin (n 25), paras. 114–18, referring to numerous factors creating a close connection to German law (which the court deemed sufficient for the purpose of Article 4(3) of the Rome II Regulation (n 21), without having even tried to establish the necessary point of reference under its Article 4(1)).

85 See Graziano (n 37), 1715–16.

In EU PIL,[86] for instance, this is particularly true for the special rules on acts of unfair competition, which shift the focus towards the affected market.[87] The rules on product liability could similarly be seen as facilitating the search for the applicable law by offering a cascade of relevant connecting factors, although the CJEU has recently reiterated that only physical objects (and electricity) can constitute a defective product (in the context of the EU Product Liability Directive),[88] independently of the harmful information it may contain.[89] For claims based on data protection law, the General Data Protection Regulation (GDPR)[90] helpfully defines its own scope of application by reference to the place of establishment of the data processor/controller.[91]

The same cannot be said for the area of IP law, though. It seems to be almost globally agreed that claims arising from infringements of IP rights must be subject to the *lex loci protectionis*.[92] Applied to infringements committed on the internet, which make content available in countless places at once, this approach quickly runs into problems. Claimants need to seek protection under countless different national laws, while defendants are exposed to liability under just as many legal systems. For infringements committed in the context of a blockchain that is automatically and unalterably stored on a decentralised network of computers, potentially requiring global enforcement of a

86 In addition to the rules for specific torts discussed in this paragraph, this is also true for other non-contractual obligations, for which Articles 10–12 of the Rome II Regulation (n 21) shift the focus towards the putative or pre-existing relationship between the parties (if there is any).

87 See *id.*, Articles 6(1), (3).

88 Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, [1985] OJ L210/29. According to the Explanatory Memorandum of the Rome II Regulation (COM(2003) 427 final, 2003/0168 (COD), 13), the definition of the Directive also applies to the Rome II Regulation (*contra* Piotr Machnikowski, "Article 5 Rome II Regulation," in Ulrich Magnus and Peter Mankowski (eds), *ECPIL: Rome II Regulation* (Cologne: Otto Schmidt 2019), paras. 26–27).

89 Judgment of the Court (First Chamber) of 10 June 2021, *VI v KRONE – Verlag Gesellschaft mbH & Co KG*, Case C-65/20 (ECLI:EU:C:2021:471).

90 GDPR (n 27).

91 See *id.*, Article 3. On the question of whether Article 3 also governs the applicable law in areas in which the Regulation defers to the individual member states, see Merlin Gömann, *Das öffentlich-rechtliche Binnenkollisionsrecht der DS-GVO* (Tübingen: Mohr Siebeck 2021), 529–738.

92 See Paul Goldstein and Bernt Hugenholtz, *International Copyright. Principles, Law, and Practice* (Oxford: Oxford University Press 2010), 138. See also Article 8 of the Rome II Regulation (n 21), which according to Recital (26) of the Regulation preservers the "universally acknowledged principle of the *lex loci protectionis*."

given IP right, these problems are emphasised even more. With distributed ledger technology now also being actively discussed as a potential solution for the administration of copyright-protected works and their protection against online piracy,[93] it remains highly unfortunate that the proposed alternatives to the *lex loci protectionis* rule[94] have so far failed to gain traction outside of academia.[95]

6 Party Autonomy

In the interest of painting a complete picture, it should be mentioned that to the extent that PIL systems carve out a role for party autonomy in tort law,[96] a party choice of law might – in theory – also be possible in certain situations involving crypto assets.[97] Except for torts committed within a system of consensus rules that already include at least an implicit choice of law (which, as shown above, might also be taken into account in other ways),[98] it is highly unlikely that the participants in a decentralised and usually pseudonymous network select the applicable tort law.[99]

7 *Lex Cryptographia*

As with many other innovations in the context of the internet,[100] the proposal has been made to abandon the conflict-of-laws analysis altogether and instead

93 See, *e.g.*, Sebastian Pech, "Copyright Unchained: How Blockchain Technology Can Change the Administration and Distribution of Copyright Protected Works" (2020) 14 Northwestern Journal of Technology and Intellectual Property 1, 1 et seq.

94 See, *e.g.*, European Max-Planck Group on Conflict of Laws in Intellectual Property (CLIP), *Principles on Conflict of Laws in Intellectual Property* (CLIP 2011), Article 3:603; American Law Institute, *Intellectual Property: Principles Governing Jurisdiction, Choice of Law, and Judgments in Transnational Disputes* (American Law Institute 2008), § 321. See also Lutzi (n 43), paras. 5.163–172.

95 See, *e.g.*, *Pez Hejduk* (n 51), confirming a similar approach with regard to international jurisdiction.

96 See, *e.g.*, Article 14 of the Rome II Regulation (n 21).

97 See Guillaume (n 47), 70.

98 See *supra* section 4. See also Peter Mankowski, "Article 14 Rome II Regulation," in Ulrich Magnus and Peter Mankowski (eds), *ECPIL: Rome II Regulation* (Cologne: Otto Schmidt 2019), paras. 17–19.

99 See also Lehmann (n 3), paras. 148–49.

100 For a short overview of this line of thought, see Lutzi (n 43), paras. 2.14–15.

directly apply the consensus rules and similar norms that govern the crypto network in question as the *lex cryptographia*.[101]

While there certainly are some conceptual arguments that seem to support this proposal,[102] especially where it focuses more on overcoming flaws of traditional legal systems than on replacing them altogether, subjecting torts against crypto assets exclusively to a perceived *lex cryptographia* would not only clash with the discipline's traditionally strong focus on state law[103] but would also be subject to the same pertinent criticism that has prevented the *lex informatica* and similar constructs from ever gaining recognition as a serious alternative to state law.[104] The fragmented and opaque nature of such systems is especially pronounced in the case of crypto networks.[105] In addition, it would certainly be very difficult to find a legal basis for a direct application of the *lex cryptographia* in tort cases – on which it would rarely provide much guidance anyway.

Once again, this does not mean that PIL requires courts to completely ignore the normative context of a tort. *Au contraire*, it has long been acknowledged that identifying the applicable law does not prevent courts from considering rules that are part of a different legal system as "local data," which are part of the relevant matrix of facts.[106] For torts that are committed within the normative environment of a crypto network, for example through intentional violation or manipulation of the consensus rules, these rules must evidently be part of the analysis, regardless of whether or not these rules can be considered a legal system on their own.

---

101 See Guillaume (n 47), 71–75; Carla L Reyes, "Conceptualizing Cryptolaw" (2017) 96 Nebraska Law Review 384, 384 et seq; Aaron Wright and Primavera De Filippi, "Decentralized Blockchain Technology and the Rise of Lex Cryptographia" (*SSRN*, 10 March 2015) <http://dx.doi.org/10.2139/ssrn.2580664>.

102 See Lutzi (n 43), paras. 5.131–33.

103 As to which see Ralf Michaels, "The Re-state-ment of Non-State-Law: The State, Choice of Law, and the Challenge from Global Legal Pluralism" (2005) 51 Wayne Law Review 1209, 1228–31; Pierre Mayer, "Le phénomène de la coordination des ordres juridiques étatiques en droit privé" (2007) 327 Recueil des cours, para. 39.

104 See Lutzi (n 43), paras. 5.134–38.

105 See also Lehmann (n 3), paras. 50–51.

106 See Tim W Dornis, "Local Data," in Jürgen Basedow et al. (eds), *Encyclopedia of Private International Law* (Cheltenham/Northhampton: Edward Elgar 2017), 1166; see also Lutzi (n 43), paras. 5.147–49. This approach is reflected in Article 17 of the Rome II Regulation (n 21).

8 Conclusion

The protection of crypto assets provides an interesting test case for the traditional PIL rules in tort. It highlights the difficulty of localising pure economic loss, especially where it takes place within a decentralised, virtual environment, simultaneously stored on countless computers all around the globe.

At the same time, the problem emphasises the potential of two connecting factors, which will only become more relevant as our lives are spent increasingly online: first, the place of acting, which not only avoids many of the uncertainties involved in finding the place of the damage and often points to an applicable law that is both predictable and closely connected to the case at hand; and, second, an open-textured escape clause, which reflects the fact that a growing number of torts happen within environments that can be linked to a particular legal system. As in other online cases, trying to find the legal system that best reflects the parties' expectations as to the legal norms governing their behaviour in a seemingly virtual world arguably remains a more promising enterprise than trying to localise assets that are inherently delocalised.

CHAPTER 15

International Insolvency Law and Cryptocurrencies

Giovanni Maria Nori and Matteo Girolametti

1 Philosophy of Money and Cryptocurrencies*

John Maynard Keynes wrote that the history of money begins with Solon, "… the first statesman whom history records as employing the force of law to fit a new standard coin to an existing money of account."[1] The president of the European Central Bank (Christine Lagarde) reminds us that the defence of a currency is still an affair of state (or of the central bank of the latter),[2] and on 9 September 2019 highlighted that "Euro is a European public good."[3] Although, notably,

* Dr. Giovanni Maria Nori authored sections 1 and 2 of this paper; Matteo Girolametti authored sections 3, 4 and 5.

1 John Maynard Keynes, *The Collected Writings of John Maynard Keynes: Volume 28, Social, Political and Literary Writings*, Elizabeth Johnson and Donald Moggridge (eds) (CUP 2012), 226.

2 On this topic, see Benjamin Klein, "The Competitive Supply of Money," (1974) 6 Journal of Money, Credit and Banking 423, who states that: "few areas of economic activity can claim as long and unanimous a record of agreement on the appropriateness of governmental intervention as the supply of money."

3 See Annex N. 2 of the Report on the Council recommendation appointing the President of the European Central Bank (N9-0023/2019 – C9-0048/2019 – 2019/0810(NLE)), available at: <https://www.europarl.europa.eu/doceo/document/A-9-2019-0008_IT.html> accessed 27 October 2022. On this point, see the Treaty on the Functioning of the European Union, [2012] OJ C326/1 ("TFEU"), Art. 282 "1. The European Central Bank, together with the national central banks, shall constitute the European System of Central Banks (ESCB). The European Central Bank, together with the national central banks of the Member States whose currency is the euro, which constitutes the Eurosystem, shall conduct the monetary policy of the Union. 2. The ESCB shall be governed by the decision-making bodies of the European Central Bank. The primary objective of the ESCB shall be to maintain price stability. Without prejudice to that objective, it shall support the general economic policies in the Union in order to contribute to the achievement of the latter's objectives. 3. The European Central Bank shall have legal personality. It alone may authorise the issue of the euro. It shall be independent in the exercise of its powers and in the management of its finances. Union institutions, bodies, offices and agencies and the governments of the Member States shall respect that independence. 4. The European Central Bank shall adopt such measures as are necessary to carry out its tasks in accordance with Articles 127 to 133, with Article 138, and with the conditions laid down in the Statute of the ESCB and of the ECB. In accordance with these same Articles, those Member States whose currency is not the euro, and their central banks, shall retain their powers in monetary matters. 5. Within the areas falling within its responsibilities, the

© GIOVANNI MARIA NORI AND MATTEO GIROLAMETTI, 2023 | DOI:10.1163/9789004514850_017
This is an open access chapter distributed under the terms of the CC BY-NC-ND 4.0 license.

pursuant to art. 282 TFEU, said Bank is certainly not subject to the powers of the Member States, because "Union institutions, bodies, offices and agencies and the governments of the Member States shall respect that independence."

By contrast, virtual currencies have generated a real "private" and anarchic monetary system, in defiance of that state "patent", idealised by Georg Simmel in his famous work (Philosophy of money), concerning the exclusive right to mint money.[4] We note that this "patent" has been questioned several times in the course of history, with reference to the so-called alternative currencies.[5]

Before delving into these new legal horizons, perhaps today this new virtual monetary system has (really) challenged the idea of a state "patent" as expressed by George Simmel, except that this epilogue (or this beginning, depending on one's point of view) appears to be consistent with the idea of Simmel's "patent" since, sooner or later, all patents – by nature – tend to capitulate in the face of the progress of a new technology. And therefore, perhaps, the issue that deserves more attention, from a scientific (juridical-economic) point of view, is not so much the overcoming of the state money minting exclusivity. Rather, the aspect that needs to be stressed is the development of a new currency (indeed virtual) unanchored to a specific causal need, a need that instead is typically the basis of all the non-virtual alternative currencies known to date. In addition, these virtual currencies are not defended by any "sword" or sovereign law, but are, instead, based on an anarchist system without any authoritative and/or legislative imposition.

Before even outlining the legal features of these new entities, it is necessary to analyse the current world economic development of this virtual monetary system (if it can be described as such), given that the most famous cases of alternative currencies (we are thinking of the Brixton pound), have often had a rather limited economic distribution, both in time and space, since alternative currencies stem from, and are linked to, a specific place and historical moment (characterised, for example, by a war, a famine or other reasons). In particular, it is possible to refer for example to the Depression Scrip, a subspecies of debt security that circulated in some areas of the United States (geographical limit) during the Great Depression (1930s, time limit) to cope with the drastic decrease of circulating liquid assets (causal connection limit).[6]

European Central Bank shall be consulted on all proposed Union acts, and all proposals for regulation at national level, and may give an opinion."

4 Georg Simmel, *The Philosophy of Money*, David Frisby (ed) (2nd edn, Routledge 1990), 294.

5 On this issue, see Garrick Hileman, "A History of Alternative Currencies" (*Hillsdale*, last updated 29 October 2014), 8 et seq. <https://www.hillsdale.edu/wp-content/uploads/2016/02/FMF-2014-A-History-of-Alternative-Currencies.pdf>.

6 Joel William Canaday Harper, *Scrip and Other Forms of Local Money* (University of Chicago 1948).

On the contrary, cryptocurrencies are a global phenomenon (there are no geographical limits) and do not even seem to be temporally limited, given that the first bitcoin exchanges date back to 2009; today they are regularly traded (along with thousands of other virtual currencies) 24 hours a day, 7 days a week, on hundreds and hundreds of exchanges (no time limit). In addition, it should be noted that cryptocurrencies do not exist/were not created to overcome a lack of money or liquid assets, nor to cope with extraordinary situations such as wars or famines; therefore, it would seem that a causal aspect or an intrinsic utility for the issuance of virtual currencies is completely lacking (no causal limit).

Indeed, among the various cryptocurrencies, bitcoin[7] is, undoubtedly, the most widely known and used. This is not only for "historical" reasons, given that bitcoin has been circulating for 13 years,[8] but also because of its economic relevance, as market capitalisation has now reached about € 625 billion (as of 7.5.2022).[9] Furthermore, bitcoin prominence is also due to one of the (perhaps indirect) functions of bitcoin itself, namely being a digital asset with a high value (when these pages were written, a bitcoin traded at a price of approximately € 49,000.00). The fame of bitcoin is widely demonstrated by empirical market data, as the average trading volumes over 24 hours was approximately

7 The word 'Bitcoin' when capitalised refers to the Bitcoin network or protocol. On the other hand, the word 'bitcoin' beginning with a lower-case letter identifies the currency (also known as 'BTC' or 'XBT'). For more information, see bitcoin, "Some Bitcoin words you might hear" (*bitcoin*) <https://bitcoin.org/en/vocabulary#bitcoin> accessed 27 October 2022 and "Bitcoin" (*Bitcoin Wiki*) <https://en.bitcoin.it/wiki/Bitcoin> accessed 27 October 2022.

8 When an anonymous author, known under the pseudonym of Satoshi Nakamoto published an article entitled: *Bitcoin: A Peer-to-Peer Electronic Cash System* (Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (*Bitcoin*) <https://bitcoin.org/bitcoin.pdf> accessed 27 October 2022).

9 It should be noted that on 1.10.2018, the market capitalisation of bitcoin was $114 billion, approximately 17 million units of currency had been issued, and the average volume over a 24-hour period was $3,982,705,851, while the price had reached $6,598.49, whereas the market capitalisation of all digital assets totalled $222 billion, with an average 24-hour volume of $14 billion. As of today (7.5.2022), the market capitalisation of bitcoin is € 625 billion, approximately 19 million units of currency have been issued, the average volume over 24 hours is € 31 billion, while the price has reached approximately € 34,000.00, as reported by CoinMarketCap ("Today's Cryptocurrency Prices by Market Cap" (*CoinMarketCap*) <www.coinmarketcap.com> accessed 27 October 2022) and Blockchain ("The world's most popular way to buy, sell, and trade crypto" (*Blockchain*) <www.blockchain.com> accessed 27 October 2022). The market capitalisation of all virtual currencies (approximately 19332) is € 1,504,383,233,431, with a 24-hour average volume of € 93 billion, as reported in the same markets. For an economic analysis of bitcoin, see David Yermack, "Is Bitcoin a Real Currency? An economic appraisal" (*NBER*, December 2013) <www.nber.org/papers/w19747> accessed 27 October 2022; Giuliano Lemme and Sara Peluso, "Criptomoneta e distacco dalla moneta legale: il caso bitcoin," (2016) 4 Rivista di Diritto Bancario 1, 1.

€ 47 billion.[10] Moreover, there are some key exogenous and endogenous factors concerning bitcoin itself that have facilitated its distribution, and which can be summarised as follows:

a The risk of devaluation of traditional currencies due to an expansive macroeconomic monetary policy, put into place by all the major central banks (US, European and Japanese) in recent years;[11]

b The risk of a sudden, explosive and unstoppable inflation due to the aforementioned monetary policy, given that this attitude of the central banks has in fact created the conditions for a market with negative interest rates. Therefore, the appetite shown by the market for assets such as bitcoin is not surprising, given bitcoin's deflationary nature. Indeed, bitcoin - unlike legal tender coins - can be "minted" in a limited way, since the total number of such cryptocurrency units will never exceed the limit of 21 million by coding of the Bitcoin protocol itself (and the same is true for several cryptocurrencies: ripple, litecoin, bitcoin cash, etc.).[12] Therefore, bitcoin is a "scarce" commodity, like other goods such as copper, oil and gold;[13]

c The lower cost of managing, storing and exchanging bitcoin (transaction fees) compared to the more traditional storage of value goods (mainly gold, and other precious commodities);

d The diversification of the investment portfolio. In this regard, cryptocurrencies in general (not just bitcoin) represent an alternative to traditional financial assets (bond market, stock market, commodities market, etc.), as well unregulated assets, and are therefore less subject to political risks or those related to international relations (wars, diplomatic crises, *etc*.). However, this does not mean that they are free from some issues. On the contrary, there are many inherent risks of cryptocurrencies, such as

10 For additional detail see (n 9).

11 Distrust of traditional currencies has always been a growth factor, initially of bitcoin, and subsequently for cryptocurrencies in general. On this point, see John McGinnis and Kyle Roche, "Bitcoin: Order without Law in the Digital Age," Northwestern Public Law Research Paper No. 17–06 (last revised 18 April 2019) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2929133>).

12 Bitcoin limit of units will presumably be reached in 130 years, as the number of bitcoin mined by solving the calculations necessary for the creation of a block is halved every 4 years.

13 Equivalence operated by the US Commodity Futures Trading Commission, as recalled by certain authors: Giovambattista Palumbo, "Il trattamento tributario dei bitcoin," (2016) Diritto e pratica tributaria 286, 290–291.

volatility (excluding stablecoins),[14] theft, loss of physical support, market abuse due to the absence of regulation and insolvency of trading platforms.[15]

Thus, it is clear that cryptocurrencies (and in particular bitcoin) have benefited from an environment favourable to their proliferation, and that this "habitat" has guaranteed such digital assets a much wider distribution (in geographical and temporal terms) than any other currency or alternative currency. In addition, it should be remembered that the most remarkable dissimilarity between legal tender currencies and cryptocurrencies consists of the absence of central authority or an issuing institution. For example, the bitcoin creation system is based on a so-called "mining" procedure, in which the various members of the network, on the basis of a peer-to-peer consensus mechanism, provide their computational power to solve a certain number of calculations necessary before a new block for the blockchain can be propagated on the network.[16]

---

14 On the risk of volatility and consequent market abuse, see Roy Kediar and Stéphane Blemus, "Cryptocurrencies and Market Abuse Risks: It's Time for Self-Regulation" (*SSRN*, 25 February 2018) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3123881>. On the issue of stablecoins, see Lael Brainard, "Digital Currencies, Stablecoins, and the Evolving Payments Landscape" (*Federal Reserve* 16 October 2019) <www.federalreserve.gov/newsevents/speech/brainard20191016a.htm>; Dirk Bullmann, Jonas Klemm and Andrea Pinna, "In Search for Stability in Crypto-assets: are Stablecoins the Solution?" (*ECB*, August 2019) <https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op230~d57946be3b.en.pdf> accessed 27 October 2022.

15 On the general risks relating to cryptocurrencies, please refer to: Giovanni Maria Nori, "Bitcoin, tra moneta e investimento," (2021) 1 Banca Impresa Società 179, fn. 91; Lael Brainard, "Cryptocurrencies, Digital Currencies, and Distributed Ledger Technologies: What Are We Learning?" (*Federal Reserve*, 15 May 2018) <www.federalreserve.gov/newsevents/speech/brainard20180515a.htm>; Richard Hennecke, "Darf ich in Bitcoin zahlen? - Geldwäscherisiken für Industrie- und Handels-Unternehmen bei Bitcoin-Transaktionen," (2018) CCZ 120 et seq.; Anastasia Sotiropoulou, "Brèves réflexions sur la réglementation des monnaies virtuelles," (2018) 4 Bulletin Joly Bourse 224 et seq.; Puente González, "Criptomonedas: naturaleza jurídica y riesgos en la regulación de su comercialización," (2018) 22 Revista de derecho del mercado de valores 5; Roberto Bocchini, "Lo sviluppo della moneta virtuale," (2017) 33 Diritto dell' informazione e dell' informatica 27, 33 et seq.; Marco Krogh, "Transazioni in valute virtuali," (2018) 2 Notariato IPSOA, 155 et seq.; Michele Bellino, "I rischi legati all'ecosistema bitcoin," (2018) 30 Rivista di Diritto Bancario; Novella Mancini, "Bitcoin: rischi e difficoltà normative," (2016) 1 Banca impresa e società, 111 et seq.

16 On the characteristics and potentiality of blockchain, see Philipp Paech, "The Governance of Blockchain Financial Networks," (*SSRN*, 6 December 2017) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2875487>; Melanie Swan, *Blockchain. Blueprint for a New Economy* (Sebastopol: O'Reilly 2015), 3 et seq.; Dirk Zetzsche, Douglas W. Arner and Ross Buckley, "The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain,"

It should be recalled that cryptocurrencies can also be purchased by exchanging legal tender currency or other cryptocurrencies on specific trading platforms and/or currencies exchange, or, again, obtaining them as payment for an operation for the sale of goods or services. On this specific point, it is important to point out that, to date, companies such as Paypal, General Motors (and many others, such as Tesla)[17] have begun to accept payment in some cryptocurrencies (mainly bitcoin and ethereum), and other companies have started offering virtual currency-based services to their clients, such as the investment bank Goldman Sachs.

As far as the storage of cryptocurrencies is concerned, these can be stored both on one's personal computer and/or smartphone (using specific software), or in so-called e-wallets (online wallets) that can also be managed by third parties (wallet service providers).

On the basis of these brief introductory notes, we can now deal with the subject of the legal qualification of virtual currencies which, indeed, has

(2017) SSRN Electronic Journal 1, 10 et seq. On the topic of smart contracts, instead, see: Michele Giaccaglia, "Considerazioni su Blockchain e smart contracts (oltre le criptovalute)," (2019) 35 Contratto e Impresa 941, 941 et seq.; Giuliano Lemme, "Gli *smart contracts* e le tre leggi della robotica," (2019) 1 Analisi Giuridica dell'Economia 129, 129; Carla Pernice, "Smart contract e automazione contrattuale: potenzialità e rischi della negoziazione algoritmica nell'era digitale," (2019) 1 Diritto del mercato assicurativo e finanziario, I, 2019, 117; Giorgio Remotti, "Blockchain smart contract. Un primo inquadramento," (2020) 1 Osservatorio del diritto civile e commerciale 189, 189-228.

17 Tesla accepted bitcoin as payment until 13.5.2021, but recently Elon Musk has stated that Tesla is "*most likely*" to accept it again. See BBC, "Bitcoin climbs as Elon Musk says Tesla 'likely' to accept it again" (*BBC*, 22 July 2021) <https://www.bbc.com/news/business-57924354>.

already been the subject of extensive studies[18] and case law,[19] as well as of many analyses conducted by administrative authorities, including the German

18 The legal doctrine on this subject is wide: see Benjamin Beck, "Bitcoins als Geld im Rechtssinne," (2015) Neue Juristische Wochenschau 580, 580 et seq.; Yasutake Okano, "Virtual Currencies: Issues Remain after Payment Services Act Amended," (2016) 243 Nomura Research Institute 1; Christopher Danwerth, "The Regulation of Bitcoin and Other Virtual Currencies under Japanese Law in Comparative Perspective," (2018) 2 ZVglRWiss 117, 117 et seq.; Hanna Halaburda and Miklos Sarvary, *Beyond Bitcoin: the Economics of Digital Currencies* (New York: Palgrave Macmillan 2016); Gautier Bourdeaux, "Propos sur les « crypto-monnaies »," (2016) Revue de droit bancaire et financier 92, 92 et seq.; Esther María Salmerón Manzano, "Necesaria regulación legal del bitcoin en España," (2017) 4 Revista de Derecho Civil 293, 293 et seq.; Marco Cian, "La criptovaluta – Alle radici dell'idea giuridica di denaro attraverso la tecno-logia: spunti preliminari," (2019) 72 Banca Borsa Titoli di Credito 315, 315 et seq.; Vincenzo De Stasio, "Verso un concetto europeo di moneta legale: valute virtuali, monete complementari e regole di adempimento," (2018) 71 Banca Borsa titoli di credito 747, 747 et seq.; Vincenzo De Stasio, "Le monete virtuali: natura giuridica e disciplina dei prestatori di servizi connessi," in Marco Cian and Claudia Sandei, *Diritto del Fintech* (Milano: CEDAM 2020), 215 et seq.; Paolo Carrière, "Le 'criptovalut' sotto la luce delle nostrane categorie giuridiche di 'strumenti finanziari', 'valori mobiliari' e 'prodotti finanziari'; tra tradizione e innovazione," (2019) Rivista di Diritto Bancario 117, 117 et seq.; Carla Pernice, *Digital currency e obbligazioni pecuniarie* (Napoli: Edizioni Scientifiche Italiane 2018); Carla Pernice, "Criptovalute e bitcoin: stato dell'arte e questioni ancora aperte," in *Fintech. La finanza tecnologica* (Napoli: Edizioni Scientifiche Italiane 2019), 491 et seq.; Noah Vardi, "Criptovalute e dintorni: alcune considerazioni sulla natura giuridica dei Bitcoin," (2015) 3 Il diritto dell'informazione e dell'informatica 443; Giorgio Gasparri, "Timidi tentativi giuridici di messa a fuoco del bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?," (2015) 31 Il diritto dell'informazione e dell'informatica 415.

19 See *Skatteverket v. Hedqvist*, ECJ Case C-264/14, ECLI:EU:C:2015:718, in Foro italiano 2015, 11, IV, 513, with case note of Milena Piasente, "Esenzione IVA per i 'bitcoin': la strada indicata dalla Corte UE interpretando la nozione 'divise' [Nota a sentenza: Corte di giustizia UE, sez. V, 22 ottobre 2015, causa C-264/11]," (2016) 2 Corriere tributario 141. In the US, see *Securities and Exchange Commission v. Trendon T. Shavers and Bitcoin Savings and Trust*, 13-cv-00416 (E.D. Texas, September 18, 2014). About legal qualification of bitcoin in Italy, see: Trib. Verona, 24 January 2017, n. 195, in Banca borsa tit. Cred., 2017, 4, II, 467, with case note of Mario Passaretta, "Bitcoin: il leading case italiano," (2017) 70 Banca borsa e titoli di credito 471, 471 et seq.; TAR Lazio, 27 January 2020, n. 01077/2020, questo riferimento a diritto bancario eliminiamolo with the case note of Maria Consiglia Di Martino, "Nuova definizione di valute virtuali: l'orientamento del TAR" (*Giustizia Civile*, 10 November 2020) <https://giustiziacivile.com/banca-finanza-assicurazioni/note/nuova-definizione-di-valute-virtuali-lorientamento-del-tar>. On the topic of equity contributions of cryptocurrencies, see: Trib. Brescia, Sez. Imprese, 18.7.2018, decree n. 7556, Corte Appello Brescia, 24.10.2018, decree n. 26, eliminiamo questi richiami e lasciamo solo la mia nota a sentenza both with the case note of Giovanni Maria Nori, "Il capitale sociale virtuale.

Financial Supervisory Authority (BaFin), the US Commodity Futures Trading Commission (CFTC), the European Central Bank (ECB), the Bank of Italy,[20] CONSOB[21] and the Italian Revenue Agency.[22]

2 Legal Qualification of Cryptocurrencies in the EU Regulatory Framework

In this section, we will address the issue of the legal qualification of cryptocurrencies, within the limits of the European regulatory framework, with brief digressions concerning non-EU regulatory experiences.

Riflessioni in merito alla conferibilità delle criptovalute nel capitale sociale," (2020) 1 Riv. Dir. Mercato assicurativo e finanziario 1, 125 et seq. Concerning bankruptcy of an exchange service provider of cryptocurrencies, see Trib. Firenze, sez. Fallimentare, 21.1.2019, n.18, (stesso discorso cancellare tale richiamo e lasciare solo la nota a sentenza) with case note of Mario Passaretta, "Servizi di custodia e gestione di criptovalute: il fallimento del prestatore di servizi" (*Giustizia civile*, 10 June 2020) <https://giustiziacivile.com/societa-e-concorrenza/note/servizi-di-custodia-e-gestione-di-criptovalute-il-fallimento-del>.

20 *Comunicazione del 30 gennaio 2015 – Valute virtuali*, in *Bollettino di Vigilanza* n. 1, gennaio 2015. In this Communication it is clarified that "the so-called virtual currencies are digital representations of value not issued by a central bank or public authority. They are not necessarily linked to a legal tender currency, but are used as a means of exchange or held for investment purposes and can be transferred, stored and traded electronically. Virtual currencies are not legal tender and must not be confused with electronic money. And, again, that in Italy 'the purchase, use and acceptance of virtual currencies in payment must be considered legitimate activities by the State; the parties may choose to pay sums also not expressed in legal tender currencies." In the same document, it was also noted that "the attention to the fact that the activities of issuing virtual currency, converting legal money into virtual currencies and vice versa and managing the related operational schemes could instead imply, in the national law, the violation of provisions regulations, criminally sanctioned, which reserve the exercise of the related activity only to legitimate subjects (articles 130, 131 TUB for banking activities and savings collection activities; article 131-ter TUB for the provision of payment; art. 166 of the TUF, for the provision of investment services)."

21 Among the most recent analyses: Resolution no. 20944, Suspension, pursuant to Article 99, Paragraph 1, Subparagraph b), of the legislative decree n. 58/1998, of the offer to the public resident in Italy concerning "Liracoin" made by "Liracoin - DAMO," 2019; Resolution no. 20814, Prohibition, pursuant to Article. 99, Paragraph 1, Subparagraph d), of Legislative Decree n. 58/1998, of the public offer for investments of a financial nature promoted by Cryptoforce Ltd.

22 Resolution of the Revenue Agency of 2 September 2016, no. 72/E, pursuant to which virtual currencies are assimilated to foreign currencies for the purpose of determining tax treatment.

Cryptocurrencies, being issued neither by a central bank nor by a centralised issuer cannot be considered legal tender pursuant to art. 128 TFEU.[23] However, we can anticipate that the purchase, use and acceptance for payment of virtual currencies must, at present, be considered legitimate activities; but let us proceed in the proper order.

Even excluding the nature of legal tender, virtual currencies cannot be considered electronic currencies.[24] In fact, in terms of regulatory framework, Article 1, Paragraph 3 Subparagraph b), of Directive no. 46/2000 EC, electronic money is defined in the following way:

> electronic money shall mean monetary value as represented by a claim on the issuer which is: (i) stored on an electronic device; (ii) issued on receipt of funds of an amount not less in value than the monetary value issued; (iii) accepted as [a] means of payment by undertakings other than the issuer.[25]

This definition was then specified in Article 2 No. 2 Directive no. 110/2009 EC):

> 'electronic money' means electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions as defined in Point 5 of Article 4 of Directive 2007/64/EC, and which is accepted by a natural or legal person other than the electronic money issuer.

Having identified the relevant regulatory framework, the differences between virtual currency and electronic money emerge clearly (given that they have in common only the absence of a representative physical support):

a electronic money, pursuant to Article 2 No. 2 of the aforementioned Directive, are issued in exchange for funds of a corresponding value and expressed in legal tender currency (the euro). By contrast, virtual

23 Pursuant to Council Regulation (EC) No 974/98 of 3 May 1998 on the introduction of the euro, [1998] OJ L139/1 and the Consolidated version of the Treaty on the Functioning of the European Union, [2012] OJ L326/47 ("TFEU"), as amended by Article 2 of the Treaty of Lisbon, [2007] OJ C306/1, Article 128, the only banknotes having legal tender in the European Union are those issued by the ECB and national central banks.

24 This exclusion is agreed among scholars, see for all: De Stasio, "Verso un concetto europeo di moneta legale," (n 18), 753–754; Vardi (n 18), 445.

25 On the issue of electronic money, see Vincenzo Troiano, *Gli istituti di moneta elettronica* (Roma: Banca d'Italia 2001).

currencies are generated with the data mining procedure and/or other more specific procedures (with some exceptions such as Tether, which is generated and exchanged against payment of US dollars;

b virtual currencies are not issued by a central bank or by a centralised issuer, as they are "minted" through a system that is not regulated, nor controlled or controllable by any entity/market operator, while electronic money can only be issued and recognised by duly authorized parties pursuant to Directive 110/2009/EC (title II, the so-called "electronic money institutions"). Nevertheless, this feature is not always present: a mechanism of control is sometimes provided, as in the case of tether, which in fact is issued by a company subject to the control of the competent US authorities, or as ripple, which was recently involved in an investigation by the SEC;

c electronic money, pursuant to Article 11 of the above-cited Directive, is always redeemable in "real" legal tender currency at the request of the holder. In contrast, this mechanism does not operate for virtual currencies (and there are no exceptions), as they can be exchanged with fiat currency only through exchanges[26] that are not obliged to accept such virtual currencies. Yet, this legal "certainty" regarding the exclusion of virtual currencies from the category of electronic money gave way to the new Proposal for a Regulation of the European Parliament and of the Council on the Markets for crypto-assets and amending Directive (EU) 2019/1937 ('MiCA proposal'). In particular, this proposal introduced *ex novo* the regulation of "*electronic money tokens*" as "a type of crypto-asset the main purpose of which is to be used as a means of exchange and that purports to maintain a stable value by referring to the value of a fiat currency that is legal tender," which are legally equivalent to electronic money, given that the issuer must be authorized as a credit institution or "*institution of electronic money*" pursuant to Art. 2, No. 1, of Directive 2009/110/EC, and must meet the requirements applicable to electronic money institutions referred to in Titles II and III of Directive 2009/110/EC.

Based on these considerations, it seems legitimate to ask whether virtual currencies can, at least in the abstract, fulfil the function of complementary currency not being legal tender. In order to answer this question, it is necessary to verify whether virtual currencies are able to perform the functions of

26 Exchanges are platforms, operating according to decentralised or centralised models, and which are exchange and trading systems, but are not, pursuant to the MiFID discipline, authorised trading venues, *i.e.*, regulated markets (RM), multilateral systems trading facilities (MTF) or organised trading facilities (OTF).

money, namely, according to the functional theory, those of: a) unit of account; b) means of payment (or exchange); and c) store of value.

In this regard, in the opinion of the Authors (based on the existing legal framework), it does not appear possible to recognise the characteristics and functions of money in virtual currencies, as these are not able to fulfil all three aforementioned functions. Indeed, in Europe the unit of account, pursuant to Article 4 of Reg. No. 974/1998 EC, is exclusively the euro, and more precisely: 'the euro shall be the unit of account of the European Central Bank (ECB) and of the central banks of the participating Member States', even if this regulation establishes this principle limited to the aforementioned subjects (ECB and central banks of the participating Member States), and not to other private subjects, who would be free to also adopt different units of account.[27] On this topic, we refer to a decision of the Italian Supreme Court (no. 25837/2011), which underlined the hierarchy of sources in monetary matters. In particular, the Italian Supreme Court stated that:

> shall be qualified as currency only the means of payment, universally accepted, which is an expression of the public powers of issue and management of economic value, in accordance with the objectives established by national and supranational law.[28]

In this framework of uncertain boundaries, it would seem useful to make reference, again in relation to the issue we are analysing, to some considerations that have emerged within the Court of Justice of the European Union (CJEU). According to the decision of 22.10.2015, C. 264/14 of the CJEU, bitcoin has been equated to a "contractual means of payment."[29] In particular, the CJEU, which had been called upon to rule on whether or not the exchange transactions between Bitcoin and "traditional" currencies are subject to value added tax, in a nutshell,[30] defined Bitcoin as a "contractual means of payment, or rather

27 This "lack" of virtual currencies has also been underlined by scholars. See De Stasio, "Verso un concetto europeo di moneta legale," (n 18), 756 et seq.; Krogh (n 15), 158, who states: "[e]xcluding, therefore, the possibility that virtual currencies can fall into the legal category of 'legal currencies,' all that remains is to include them in the more generic category of 'goods', in the broad meaning of Article 810 of the Italian Civil Code […]."

28 *Accord*: Italian Supreme Court, decision of 2.10.2011, no. 25837, with a case note of Luciano Ciafardini, "Offerta di prodotti finanziari mascherata da emissione di moneta: lo stop della Cassazione," (2012) 1 Giustizia civile 29, 31, with regard to the case of the "currency of the Republic of the Earth" called "dhana" (which, however, was not a virtual currency).

29 *Skatteverket* (n 19).

30 For a more detailed analysis of this ruling, see Palumbo (n 13), 279; Piasente (n 19), 141.

a direct payment method between the operators who accept it," and consequently, the provision of services which have as their object the exchange of the virtual currency against units of fiat money and vice versa, are considered exempt from VAT. Nonetheless, this qualification as a means of payment has been opposed, both by certain legal doctrine and by the ECB, as specified below.[31]

From this point of view, virtual currencies can be considered a means of payment only among the operators who accept them. Therefore, the debtor will be able to fulfil his obligation by paying in cryptocurrencies rather than in currency having legal tender only if the creditor consents.[32] Thus, there is still the possibility of refusing to accept virtual currencies in payment of a debt. The ruling in question, indeed, does not allow *ipso jure* the equivalency of cryptocurrencies and currencies not having legal tender status. However, these guidelines are limited to the tax issues of the case, and therefore do not "generally attribute the monetary character to virtual currencies."[33] In other words, and recalling the typical functions of money, virtual currencies are not legally recognised as a unit of account (at least by the ECB and central banks of the participating Member States), as they would appear to be a means of payment, or, at most, a means of exchange.

In this regard, in fact, it is worth recalling the scope and content of the provisions of the ECB opinion of 12.10.2016 (signed by Mario Draghi).[34] The ECB, referring to virtual currencies, stresses that "they are not legally established as money nor are they legal tender issued by central banks and other public authorities." And again, in the same opinion, the ECB criticises the definition

31 In this regard, however, it should be noted that scholars do not consider "applicable the rules on payment systems envisaged for example by Directive 64/2007/EC (the so-called PSD Directive) since electronic money is excluded from its scope, if he deduces by analogy, the *a fortiori* inapplicability for virtual currencies (without those forms of issue surveillance to which the first is subjected)," as said in these terms by Noah Vardi (n 18), 446–447. See also Giorgio Gasparri (n 18), 31.

32 As argued in the legal doctrine by: Massimo Giuliano, *L'adempimento delle obbligazioni pecuniarie nell'era digitale: dalla moneta legale alla moneta scritturale e digitale legalmente imposta*, (Torino: Giappichelli 2018), 134 et seq.; Giorgio Gasparri (n 18), 416 fn. 6.

33 In these terms De Stasio, "Verso un concetto europeo di moneta legale," (n 18), 755. The author argues that the judgment of ECJ is limited only to the tax issues of the said case.

34 The opinion is available at Opinion of the European Central Bank of 12 October 2016 on a proposal for a directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/10/EC (CON/2016/49), [2016] C 459/3 <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv%3AOJ.C_.2016.459.01.0003.01.ITA&toc=OJ%3AC%3A2016%3A459%3ATOC> accessed 27 October 2022.

of virtual currencies as means of payment, since "virtual currencies cannot qualify as currencies" from the point of view of the Union and indeed, in the view of the Authors, Article 2, Paragraph a), of Directive 2014/62/EU of the European Parliament and of the Council of 15 May 2014 would not seem to include virtual currencies.[35] Furthermore, the ECB clarifies that "In compliance with the Treaties and the provisions of Regulation (EC) no. 974/98 of the Council, the euro is the single currency of the economic and monetary union of the Union, that is of the member states that have adopted it as their currency." So the European Banking Authority:

> recommends defining virtual currencies more specifically, in order to explicitly clarify that virtual currencies do not constitute legally established currency or money "considering that" virtual currencies are not actually currencies, it would be more appropriate to consider them as a means of exchange rather than a means of payment.

This opinion of the ECB was not the first pronouncement of the Authority. In fact, there had already been a previous publication by that bank, titled the *Virtual Currency Schemes* (dating back to October 2012), where the virtual currency was defined as "a virtual currency [which] is a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community." The ECB added the clarification that "[t]his definition may need to be adapted in future if fundamental characteristics change."[36]

The same can be said of the Bank for International Settlements, which had already issued its own opinion (in 2015),[37] through which it had tried to draw a line between e-money and digital currencies.

However, unlike traditional e-money, digital currencies are not a liability of an individual or an institution, nor are they backed by an authority. Furthermore, they have no intrinsic value and, as a result, they derive value only from the belief that they might be exchanged for other goods or services, or a certain amount of sovereign currency, at a later point. Accordingly, holders of digital

35 Whereby currency is meant: "banknotes and coins whose circulation is legally authorized, including banknotes and coins whose release into circulation is legally authorized pursuant to Regulation (EC) no. 974/98."

36 Opinion available on the ECB website, at European Central Bank (ECB), "Virtual Currency Schemes" (*ECB*, October 2012) <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf> accessed 27 October 2022.

37 Committee on Payments and Market Infrastructures, "Digital currencies" (*BIS*, November 2015) <https://www.bis.org/cpmi/publ/d137.htm> accessed 27 October 2022.

currency may face substantially greater costs and losses associated with price and liquidity risk than holders of sovereign currency.

Some cryptocurrencies however do not "technically" have an intrinsic value equal to zero; for example, bitcoin or litecoin - from a purely accounting point of view - are worth at least the cost necessary for their production and exchange (very high in the case of the bitcoin mining), a value that increases due to the scarcity of these currencies (according to the general supply-demand mechanism) and their usefulness (for instance, the value of bitcoin appreciates every time a private entity, or an institution or a State recognises its legal validity). These considerations, reverting to the three functions of money, suggest that the requirement of the "store of value" is attributable at least to some cryptocurrencies.

In the wake of the aforementioned opinion of the ECB of 12.10.2016, the European regulatory framework has also recently been enriched by Directive no. 843/2018 EU. With this Directive (in the "recitals", Paragraph n. 10), it was preliminarily clarified what virtual currencies are not:

> Virtual currencies should not to be confused with electronic money as defined in point (2) of Article 2 of Directive 2009/110/EC of the European Parliament and of the Council, with the larger concept of "funds" as defined in point (25) of Article 4 of Directive (EU) 2015/2366 of the European Parliament and of the Council, nor with monetary value stored on instruments exempted as specified in points (k) and (l) of Article 3 of Directive (EU) 2015/2366, nor with in-games currencies, that can be used exclusively within a specific game environment. Although virtual currencies can frequently be used as a means of payment, they could also be used for other purposes and find broader applications, such as a means of exchange, investment, store-of-value products or for use in online casinos. The objective of this Directive is to "cover all the potential uses of virtual currencies."

The following assumptions are then confirmed:

i. virtual currencies are not electronic money pursuant to Article 2, Point 2, of Directive 2009/110/EC;
ii. virtual currencies are not payment instruments pursuant to EU Directive 2015/2366 (so-called PSD 2, Payment Services Directive);
iii. virtual currencies, in addition to being used as a means of payment, can also be used as a means of exchange and investment or products of store of value.

After that, and again according to the Directive in question (which would seem to have adhered to the theses of the ECB), virtual currencies are defined as:

> a representation of digital value that is not issued or guaranteed by a central bank or a public body, it is not necessarily linked to a legally established currency, it does not have the legal status of currency or money, but it is accepted by natural and legal persons as a medium of exchange and can be transferred, stored and exchanged electronically.[38]

And at the same time, a definition was also given of the subjects who carry out the activities of digital wallet service providers, such as subjects who provide: "services for safeguarding private cryptographic keys on behalf of their customers, in order to hold, store and transfer virtual currencies."

2.1 *The EU Proposed "Regulation on Markets in Crypto Assets": New (Un)certainties*

The regulatory framework described thus far was shaken by the Proposal for a Regulation of the European Parliament and of the Council on the "Markets for crypto-assets and amending Directive (EU) 2019/1937."[39] This proposal radically changes the legal landscape discussed up to this point; it also seems to include one of the most problematic aspects (in terms of regulation and legal qualification) of cryptocurrencies,[40] namely that of stablecoins, abandoning the "certainty" that "virtual currencies should not be confused with electronic money as defined in Point 2 of Article 2 of Directive 2009/110/EC."[41]

More specifically, it should be noted that among the objectives set by the European legislator (legal certainty, support of technological innovation, consumer protection) we find that of financial stability,[42] and, in particular, it is

38 Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU, [2018] OJ L156/43.

39 Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, [2020] COM/2020/593 final ("MiCA Proposal").

40 Concern arising within the G7 Working Group on stablecoins. See the report from the G7 Working Group on Stablecoins, "Investigating the impact of global stablecoins" (*BIS*, October 2019) <https://www.bis.org/cpmi/publ/d187.pdf> accessed 27 October 2022.

41 Directive (EU) 2018/843 (n 38), Recital 10.

42 The introductory report of the MiCA Proposal (n 39) states: "The first objective is one of legal certainty. For crypto-asset markets to develop within the EU, there is a need for

said that "the proposal includes safeguard measures to address the potential risks to financial stability and orderly monetary policy that could arise from stablecoins."[43]

In any case, this regulation clarifies, in Article 2 (2), that it is not intended to apply to crypto assets that qualify as: (a) financial instruments as defined in Article 4(1), point (15), of Directive 2014/65/EU;[44] (b) electronic money as defined in Article 2, Point (2), of Directive 2009/110/EC, except where they qualify as electronic money tokens under this Regulation; (c) deposits as defined in Article 2(1), Point (3), of Directive 2014/49/EU of the European Parliament and of the Council; (d) structured deposits as defined in Article 4(1), point (43), of Directive 2014/65/EU; or (e) securitization as defined in Article 2, Point (1), of Regulation (EU) 2017/2402 of the European Parliament and of the Council.

The MiCA proposal (Article 3 Paragraph 2) has not only an objective exclusion, but also a subjective one, given that it cannot be applied to: (a) the European Central Bank, national central banks of the Member States when acting in their capacity as monetary authority or other public authorities; (b) insurance undertakings or undertakings carrying out the reinsurance and retrocession activities as defined in Directive 2009/138/EC of the European Parliament and of the Council when carrying out the activities referred to in that Directive; (c) a liquidator or an administrator acting in the course of an insolvency procedure, except for the purpose of Article 42; (d) persons who provide crypto asset services exclusively for their parent companies, for their subsidiaries or for other subsidiaries of their parent companies; (e) the European investment

a sound legal framework, clearly defining the regulatory treatment of all crypto-assets that are not covered by existing financial services legislation. The second objective is to support innovation. To promote the development of crypto-assets and the wider use of DLT, it is necessary to put in place a safe and proportionate framework to support innovation and fair competition. The third objective is to instil appropriate levels of consumer and investor protection and market integrity given that crypto-assets not covered by existing financial services legislation present many of the same risks as more familiar financial instruments. The fourth objective is to ensure financial stability. Crypto-assets are continuously evolving. While some have a quite limited scope and use, others, such as the emerging category of 'stablecoins', have the potential to become widely accepted and potentially systemic. This proposal includes safeguards to address potential risks to financial stability and orderly monetary policy that could arise from 'stablecoins'."

43 MiCA Proposal (n 39), explanatory memorandum.

44 This is because (as clarified in Recital 6 of the present MiCA Proposal (n 39)): "Union legislation on financial services should not favour one particular technology. Crypto assets that qualify as 'financial instruments' as defined in Article 4(1), Point (15), of Directive 2014/65/EU should therefore remain regulated under the general existing Union legislation, including Directive 2014/65/EU, regardless of the technology used for their issuance or their transfer."

bank; (f) the European Financial Stability Facility and the European Stability Mechanism; or (g) public international organisations.

The MiCA proposal also includes several definitions. Specifically, it defines as "crypto-asset": "a digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology"; as an "asset-linked token": "a type of crypto asset that purports to maintain a stable value by referring to the value of several fiat currencies that are legal tender, one or several commodities or one or several crypto assets, or a combination of such assets"; as "electronic money token": "a type of crypto asset the main purpose of which is to be used as a means of exchange and that purports to maintain a stable value by referring to the value of a fiat currency that is legal tender"; as a "utility token": "a type of crypto-asset which is intended to provide digital access to a good or service, available on DLT, and [which] is only accepted by the issuer of that token." The proposal also outlines, in a specific and articulated way, a list of possible services that can be provided by crypto asset service providers; nevertheless, it should be noted that such a topic is beyond the scope of this paper.[45]

It is also important to stress that the MiCA proposal provides a distinction among different types of crypto assets: utility tokens (also providing a legal framework on offering and regulation), stablecoins (electronic money tokens and tokens linked to assets) and investment tokens, which are characterised as financial instruments (thus subject to the discipline referred to in Article 4, Paragraph 1, Point No 15, of Directive 2014/65/ EU). Going into more depth, each of these tokens has its own discipline; on this point, it is interesting to note that the regulatory aspects of this proposal would not seem to apply to cryptocurrencies (strictly speaking, such as bitcoin, litecoin, *etc.*), since the latter do not have an issuer that legally offers them on a platform. Such a conclusion tallies with Article 4 (2) Subparagraph b) of the proposal for a Regulation, which expressly provides for the exemption from the publication of the white paper (and other duties) for crypto assets where "the crypto-assets are

45 "[C]rypto-asset service" means any of the services and activities listed below relating to any crypto-asset: (a) the custody and administration of crypto-assets on behalf of third parties; (b) the operation of a trading platform for crypto-assets; (c) the exchange of crypto-assets for fiat currency that is legal tender; (d) the exchange of crypto-assets for other crypto-assets; (e) the execution of orders for crypto-assets on behalf of third parties; (f) the placing of crypto-assets; (g) the reception and transmission of orders for crypto-assets on behalf of third parties; (h) providing advice on crypto-assets.

automatically created through mining as a reward for the maintenance of the DLT or the validation of transactions."[46]

This circumstance confirms what has been anticipated, namely that the MiCA proposal mainly deals with the regulation of stablecoins. On this point, this regulatory initiative – in terms of the qualification of cryptocurrencies – offers an important legal innovation, given that it provides that electronic money tokens and actual electronic money may be subject to/governed by the same regulation. Therefore, stablecoins such as tether, USD coin, paxos standard and many others (which replicate the official prices of the US dollar) would, in fact, be subject to the same regulation of electronic money.

In this new *de iure condendo* framework, what is clear is the genus-to-species relationship (between crypto assets and single types of tokens) that the proposed regulation would seem to have definitively established. On the one hand, there is the "genus" represented by "Crypto assets" (*i.e.*, the digital representation of value or rights that can be transferred and stored electronically, using distributed ledger technology or a similar technology). On the other hand, it is possible to single out individual species of tokens:

a **Utility tokens**, namely the crypto assets (accepted only by the issuer) aimed at providing digital access to a good or service. Tokens that would seem to be included among the broad category of legitimation securities, given that these tokens do not even potentially have the function of money (as the specification of being accepted only by the issuer demonstrates), nor do they appear to have a financial nature since these tokens would seem to be supported – from a causal point of view – by a consumer intent as shown by Article 12 of the proposed regulation in question, when it recognises the right of withdrawal of consumers who have purchased these tokens;

b **Investment tokens**, *i.e.*, crypto assets not governed by the EU's recent MiCA proposal, but which should fall within the category of financial instruments referred to in Article 4 (1), Point No. 15, of Directive 2014/65/EU. In other words, this kind of crypto asset does not escape regulation, but the European legislator simply includes it in a previous legal text

46 The other exemptions apply when: (a) the crypto assets are offered for free; (c) the crypto assets are unique and not fungible with respect to other crypto assets; (d) the crypto assets are offered to fewer than 150 natural or legal persons per Member State where such persons are acting on their own account; (e) over a period of 12 months, the total consideration of an offer to the public of crypto assets in the Union does not exceed € 1 000 000, or the equivalent amount in another currency or in crypto assets; or (f) the offer to the public of the crypto assets is solely addressed to qualified investors and the crypto assets can only be held by such qualified investors.

(namely in that on financial instruments, the so-called MiFID II and MiFIR regime), which, moreover, is already intended to be updated in this regard.[47] Indeed, one of the most important "pieces" that make up the so-called white paper, regulated under Article 5, Point No. 7, of the MiCa Proposal, is precisely the one dedicated to illustrating the reasons why the crypto assets offered should not be considered financial instruments;

c **Asset-referenced tokens**, *i.e.*, a type of crypto asset that purports to maintain a stable value by referring to the value of several fiat currencies that are legal tender, one or several commodities (as set forth Article 2(6) of Commission Delegated Regulation (EU) 2017/565), or one or several crypto assets, or a combination of such assets. Such reserves of assets represent the underlying value of these tokens (as regulated by Articles 32 *et seq*. of the MiCA proposal), where the token buyer may not even be the holder of direct credit or reimbursement rights (see Article 25 of the MiCA Proposal on the obligation of transparency and disclosure of this condition). In such a case these tokens may be deemed financial derivative contracts (for example forwards or futures) referred to in Article 4 (1), No. 15 MiFID II, given that the speculative element would seem to prevail over the consumption element. The absence of a claim right and/or the reimbursement on reserve of activities (Article 25 MiCA Proposal), and of a right of withdrawal as well (Article 12 MiCA Proposal), are features and effects that make the token we are speaking of similar to derivative contracts of Article 4(1), No. 15 MiFID II. That is because the speculative element seems to prevail over the consumeristic one. Nonetheless, it should be noted that this article prohibits issuers from providing to the token holder interests or other benefits linked to the duration of the holding period of these tokens.

d **Electronic money tokens**, *i.e.*, crypto assets used mainly as a medium of exchange, the value of which is linked to the value of a legal tender fiduciary currency. Of all the token subspecies, this is undoubtedly the least problematic - from a qualification point of view - as it is clear that this token is in fact an electronic money, given that the issuer must be authorised as a credit institution or "institution of electronic money" pursuant to Article 2, point 1, of Directive 2009/110/EC, and must meet

47 As stated at 2 of the MiCA Proposal (n 39): "the Commission is also proposing a clarification that the existing definition of 'financial instruments' - which defines the scope of the Markets in the Financial Instruments Directive (MiFID II) - includes financial instruments based on DLT, as well as a pilot regime on DLT market infrastructures for these instruments."

> the requirements applicable to electronic money institutions referred to in titles II and III of Directive 2009/110/EC. These tokens (better known as stablecoins), have revolutionised the legal landscape of cryptocurrencies, as in their case, the position for which virtual currencies are never comparable to electronic money has been definitively abandoned, so much so that stablecoins are always redeemable by the issuer (see art. 44 of the MiCA proposal). Moreover, the issuer of these tokens is forbidden from providing remuneration to the holders in the form of interest or other benefits (art. 45), and it is evident that, given the prevalence of the exchange function for these tokens, any equality with financial instruments is excluded.[48]

In this regulatory framework, however, cryptocurrencies such as bitcoin or litecoin, are produced through data mining, but are not linked to the enjoyment of a good or service (no utility tokens), nor to the value of a currency having legal tender (no electronic money tokens or stablecoins), commodity or other, nor do they have a financial nature. It is therefore not clear under which "kind" of crypto asset these virtual currencies can be categorised.

More specifically, this type of virtual currency does not match any of the "*species*" as defined by the proposed regulation. Perhaps this is due to the fact that these cryptocurrencies could be considered property. In more precise terms, we have already mentioned the difficulty in categorising this cryptocurrency as money (including electronic money) and as a payment instrument (despite an initial case law approach to that effect).[49] Nonetheless, this difficulty helps in the attempt to find the correct qualification. In fact, it is undeniable that these virtual currencies represent a value, and as such can be considered property, given that they can be freely disposed of (spent, transferred, destroyed, *etc*.) by means of the private key. In essence, therefore, if, on the one hand, it is true that MiCA does not regulate cryptocurrencies, on the other hand, it implies - by reasoning *a contrario* - that cryptocurrencies cannot be included in any of the legal categories regulated by the MiCA proposal ("*species*"). Thus, their exclusion from these definitions allows us to corroborate the thesis that bitcoin is property, an orientation in line with

48 Moreover, the exclusion of the investment function is further demonstrated by the obligation of the issuer (pursuant to Article 49 of the MiCA Proposal (n 39)) to invest the funds received from the issuers of electronic money tokens in secure and low-risk assets, in accordance with of Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC [2009] OJ L267/7, Article 7(2).

49 See *Skatteverket* (n 19).

the non-regulation of MiCA, which in fact, provides a broad definition of the "*genus*" represented by "Crypto-assets "(*i.e.*, the digital representation of value or rights that can be transferred and stored electronically, using distributed ledger technology or a similar technology), would seem to somehow lead to this conclusion.

In this regard, we recall some cases. In the *Koinz Trading B.V.* case,[50] the District Court of Amsterdam opined that:

> Bitcoin exists, according to the court, in the form of a unique, digitally encrypted series of numbers and letters stored on the hard drive of the right-holder's computer. Bitcoin is "delivered" by sending bitcoins from one wallet to another wallet. Bitcoins are standalone value files, which are delivered directly to the payee by the payer in the event of a payment. It follows that a bitcoin represents a value and is transferable. In the court's view, it thus shows characteristics of a property right. A claim for payment in bitcoin is therefore to be regarded as a claim that qualifies for verification.

We can also refer to the USA Bankruptcy Court of the Northern District of California holding in a case on the bankruptcy of the Bitcoin mining firm HashFast's trustee (*HashFast Technologies LLC and HashFast LLC v. Marc A. Lowe*, Case No. 14-30725DM), where it was declared that bitcoins are not US dollars and should be considered as intangible property or commodities in bankruptcy procedures.[51] In other words: "Bitcoin is property, not currency."[52]

These decisions, which are far from isolated,[53] lead the interpreter to consider the idea of qualifying bitcoin (along with all the other virtual currencies not comparable to the legal categories ruled in the MiCA proposal), under the

---

50 *Koinz Trading B.V.*, Rechtbank Amsterdam, C/13/18/65 F, ECLI:EN:RBAMS:2018:869 (14 February 2018).

51 Olena Demchenko, "Bitcoin: Legal Definition and its Place in Legal Framework," (2017) 3 Journal of International Trade, Logistics and Law 23, 31 fn. 83. For the decision, see Steven C. Reingold and Timothy J. Durkin, "Bitcoins Are Not U.S. Dollars: What Does the Ruling in the HashFast Bankruptcy Mean?" available at: <http://www.jagersmith.com/downloads/pdf/Bitcoins-Are-Not-US-Dollars.pdf>.

52 Emmanuelle Inacio, "Digital Assets in Insolvency and Restructuring" (*Technical Insight*, Spring 2018) <https://www.insol-europe.org/download/documents/1509> accessed 27 October 2022.

53 See the Singapore International Commercial Court, *B2C2 Ltd v Quoine Pte Ltd*, Civil Appeal No 81 of 2019, [2020] SGCA(I) 02; the High Court of Justice of England and Wales, *AA v Persons Unknown, Re Bitcoin*, [2019] EWHC 3556 (Comm); High Court of New Zealand, *Ruscoe and Moore v Cryptopia Limited* (*In Liquidation*), [2020] NZHC 728, CIV-2019-409-000544.

category of "non-physical property rights" as increasingly well-founded and compelling.[54] This conclusion is substantially supported by several arguments.

1. As mentioned, bitcoin would not seem to be compatible with the other qualifications applicable to other types of crypto assets (utility tokens, investment tokens, asset-referenced tokens and electronic money tokens).
2. Bitcoin can be held both directly (with a physical wallet, such as a hardware wallet, named "cold wallet") and indirectly (through an e-wallet managed by specific exchange platforms, a so-called "hot wallet"). It can be kept indefinitely, and the risks of deterioration or loss are irrelevant, given that even traditional properties can be subject to this risk.
3. Bitcoin can circulate, and, in particular, it can be transferred and spent using the users' private key, and it can even be destroyed.

3. Consequences of Legal Qualification of Digital Assets in Insolvency Proceedings

After focusing on the analysis of the legal nature of crypto assets, especially cryptocurrencies, and having described the regulatory framework in the Member States of the European Union, the second part of this work will focus on the issue relating to the relationship between bankruptcy and digital assets. In particular, it is now necessary to analyse the consequences of the qualification of digital assets on insolvency proceedings and of the relationship between exchanges and clients, also in light of the MiCA proposal.

3.1 *Insolvency Estate and Property Claim in Case of Insolvency*

The first issue to tackle when analysing the application of bankruptcy law with regard to crypto assets is establishing whether the said assets can be regarded as "assets" under insolvency law, and thus be included within the insolvency estate in the event of the insolvency of a cryptocurrencies investor. In the event that the answer to this question is negative, crypto assets would not be treated as part of the insolvency estate, thereby decreasing the amount creditors may possibly recover. By contrast, if the crypto assets are deemed to be part of the

54 The same conclusion was also reached in the UK, as "cryptoassets have all the legal indicia of property and are, as a matter of English legal principle to be treated as property"; see Geoffrey Vos, "The Launch of the Legal Statement on the Status of Cryptoassets and Smart Contracts" (*Judiciary*, 18 November 2019), para. 12 <https://www.judiciary.uk/wp-content/uploads/2019/11/LegalStatementLaunch.GV_.2.pdf>.

debtor's estate, such assets would be recoverable under bankruptcy law, and the insolvency trustees should act in such a manner as to gain control over those assets in order to increase the value of the insolvency estate.

With respect to the insolvency of an individual, it is important to mention *Tsarkov,* a recent Russian case.[55] Prior to *Tsarkov*, it was unclear whether, under Russian law, crypto assets should be included in the bankruptcy estate, since their status was indeterminate. The insolvency trustee claimed that the cryptocurrencies held in a digital wallet should be deemed to be part of the debtor's assets, and therefore should be included in the insolvency estate. The court of first instance dismissed the claim. By contrast, the appellate court recognised the insolvency trustee's claim, on the grounds that cryptocurrencies should be regarded as pecuniary assets, which can be freely disposed of, used and possessed by the debtor.[56] Therefore, in the view of the Court, the debtor's status with respect to these assets should be considered similar to ownership. The Court also stressed that, cryptocurrencies having an undeniably relevant economic value, their exclusion from the insolvency estate would impede creditors from receiving full satisfaction of their claims,[57] therefore they should be deemed part of the debtor's assets. In this case, then, the Court ordered Mr. Tsarkov to give the insolvency estate administrator access to his e-wallet, so that it was possible to include cryptocurrencies among the recoverable assets for the benefit of the creditors.

The qualification of crypto assets also has serious consequences for the claims made by crypto-investors against the bankruptcy estate. Indeed, in the event of a qualification of digital assets as property, the crypto-investors would have a proprietary claim against the bankrupt, and thus would be able to claim the restitution of the digital asset having a right *in rem*. In such a case, creditors might lodge a restitution claim, thus requesting the return of the digital assets they own. Thus, the crypto assets would not be considered part of the insolvency estate, as crypto-investors have an exclusive right *in rem*.

---

55 Moscow Arbitrazh Court, Case No. A40-124668/17-71-160 (5 March 2018).

56 Decision of the 9th Appellate Court of Moscow, *Tsarkov*, Case No. A40-124668/2017 (15 May 2018).

57 For an in-depth analysis of the *Tsarkov* case decisions, see Gregory Azeff, Stephanie De Caria and Matthew McGuire, "Governing the Ungovernable: Cryptocurrencies in Insolvency Proceedings, Annual Review of Insolvency Law" (*ACFI*, 27 February 2019) <https://www.acfi.ca/2019/02/27/governing-the-ungovernable-cryptocurrencies-in-insolvency-proceedings/>. See also INSOL International, "Cryptocurrency and its Impact on Insolvency and Restructuring" (*INSOL*, May 2019) <https://www.dlapiper.com/~/media/files/news/2019/06/special-report-cryptocurrency-29-may-2019-final.pdf?la=en&hash=668F3D8499AF6A596E78DFF94B8D87FAB4C85A35> accessed 27 October 2022.

On the contrary, not qualifying crypto assets as property leads to the conclusion that such assets, not being subject to a right *in rem*, would be included in the insolvency estate. As a consequence, crypto-investors' claims would be equated to the actions of the other creditors of the bankruptcy estate, and would therefore be subject to the bankruptcy reduction, obtaining only partial satisfaction of their claims. Indeed, creditors having a right to claim will need to compete with other personal rights creditors with respect to the sum that the insolvency trustee manages to realise, pursuant to the payment priorities provided by the law applicable to the proceedings.

Proprietary issues (as opposed to contractual issues) are extremely relevant in cases where a crypto asset service provider goes bankrupt. From a contractual standpoint, if ownership over the digital assets cannot be established, users would be regarded as regular creditors and their claims on the assets would have no more priority that those of other creditors in the insolvency proceedings; and consequently would not be fully satisfied. By contrast, if users are able to prove their ownership over crypto assets, they would be entitled to the restitution of all of those assets,[58] and therefore be able to recover the same amount of cryptocurrencies as they owned.[59]

With respect to the insolvency of crypto assets exchanges, there are few cases that have recognised the proprietary qualification for cryptocurrencies. In 2018, the Supreme Court of (South) Korea[60] and the Shenzhen Court of International Arbitration[61] both found that Bitcoin was a form of property. In 2019, the Singapore International Commercial Court, in *B2C2 Ltd v Quoine Pte Ltd*,[62] also stated that Bitcoin constitutes a form of property. The High Court

58 The value of such assets, during the time necessary for the conclusion of the insolvency proceedings, will likely increase or decrease, as crypto-asset markets are highly volatile.

59 See Koji Takahashi, "Implications of Blockchain for the UNCITRAL Works" (*SSRN*, 1 May 2020) <https://ssrn.com/abstract=3566691>; Victoria Sandberg, "Regulating Cryptocurrencies in the International Insolvency Law" (*University of Turku*, June 2020) <https://www.utupub.fi/bitstream/handle/10024/150515/opinn%C3%83%C2%A4ytety%C3%83%C2%B6.pdf?sequence=1&isAllowed=y> accessed 27 October 2022.

60 See Chan Sik Ahn, "South Korea: Confiscation of Bitcoin Criminal Assets" (*IFLR*, 16 July 2018) <https://www.iflr.com/Article/3821031/South-Korea-Confiscation-of-Bitcoin-criminal-assets.html>.

61 See Wolfie Zhou, "Chinese Court Rules Bitcoin Should Be Protected as Property" (*CoinDesk*, 26 October 2018) <https://www.coindesk.com/chinese-arbitration-court-says-bitcoin-should-be-legally-protected-as-property>.

62 Singapore Court of Appeal, *B2C2 Ltd v Quoine Pte Ltd* [2019] SGHC(I) 03.

of Justice of England and Wales, in *AA v Persons Unknown, Re Bitcoin*,[63] agreed, relying for its conclusion on the Singapore case.[64]

By contrast, there is also case law concluding that restitution actions with regard to cryptocurrencies must be excluded. In 2013, MtGox Co. Ltd. (MtGox) was the biggest cryptocurrencies exchange, responsible for nearly 70% of bitcoin trades. After a hack resulting in the loss of approximately 850,000 bitcoin, MtGox filed for insolvency protection pursuant to Japanese law. In 2018, the unfinished insolvency liquidation proceeding was stayed, and a civil rehabilitation proceeding was initiated. With regard to the claim lodged by a customer asking for the return of cryptocurrencies (restitution), the District Court of Tokyo expressly concluded that Bitcoin could not be the object of ownership under Japanese law,[65] as it lacked some features necessary to be considered property.[66] However, it must be noted that, since that decision, Japan has amended its Payment Services Act, which now explicitly recognises a property right in cryptocurrencies.[67]

3.2 *Proprietary Issues and the Contractual Relationship between Exchanges and Users*

The legal nature of crypto assets is not the only relevant element to assess the nature of creditors' claims in case of insolvency of exchanges. It is also important to examine the contractual relationship between exchanges and users, as it may affect the treatment of creditors' claims.

In the *Bitgrail* case,[68] the court of first instance of Florence excluded the restitution action brought by the claimant, but on grounds other than those evoked in the aforementioned *MtGox* case. Indeed, the *Bitgrail* court held that the relationship between the users and the cryptocurrencies exchange, in the

63 *AA* (n 53).

64 More recently, the High Court of New Zealand, in *Ruscoe and Moore* (n 53), held the same view. For a detailed comment on this decision, see Paul Babie et al., "Cryptocurrencies as Property: Ruscoe v Cryptopia Ltd (in liq) [2020] NZHC 728" (2020) 28 Australian Property Law Journal 106.

65 Tokyo District Court, Judgement of Civil Division 28 of 5 August 2015, Reference number 25541521, available at <https://www.law.ox.ac.uk/sites/files/oxlaw/mtgox_judgment_final.pdf>.

66 See Matthias Haentjens, Tycho de Graaf and Ilya Kokorin, "The Failed Hopes of Disintermediation: Crypto-Custodian Insolvency, Legal Risks and How to Avoid Them," (2020) 2020 Singapore Journal of Legal Studies 526.

67 See Mai Ishikawa, "Designing Virtual Currency Regulation in Japan: Lessons from the Mt Gox Case," (2017) 3 Journal of Financial Regulation 125, 126; Gregory Azeff, De Caria and McGuire (n 57).

68 Tribunale di Firenze – sez. Fallimentare, decision N. 18/2019, published on 21.1.2019.

case at hand, was to be qualified as an "irregular deposit" pursuant to Article 1782 of the Italian Civil Code. It was not possible to ascertain whether there was a property right over the cryptocurrencies, as, after users made deposits, the Bitgrail exchange conveyed such funds to the exchange's wallet (*omnibus* address). Therefore, the exchange acquired the property right over the cryptocurrencies deposited by users in the digital wallets, maintaining the private keys and keeping the funds together at an *omnibus* address. Thus, since it was not possible to identify a property right in cryptocurrencies, Bitgrail's clients were deemed creditors of the exchange and could only issue a personal right to claim against the exchange, competing with other creditors for the satisfaction of their rights on the basis of payment priorities.

Regarding claims against a bankrupt exchange, the *Bitgrail* case demonstrates the importance of the contractual relationship between the exchange and the users. Indeed, in this case, the claim for restitution was excluded on the basis of the terms and conditions accepted by the users, as the rules (and system) provided by the exchange impeded the ability to ascribe whether Bitgrail's clients had a proprietary interest in these cryptocurrencies.

The contractual relationship between exchanges and users is therefore important to identify what kind of interest such users have in the event of insolvency of an exchange. Before delving into this matter, however, it is important to recall how the blockchain works, and, in particular, how cryptography is employed to safeguard the transactions within a given blockchain, enabling the exchange of crypto assets. Essentially, blockchains employ a system of two different types of cryptography (asymmetric-key algorithms and hash functions). The asymmetric-key algorithms consist of two mathematically-related keys, assuring a public-key encryption. Crypto assets are kept at what are called "addresses" (a line of code), identified in a blockchain. Crypto assets are moved by the sender, using its private key, sending this transaction via the network participating in the blockchain (for example the Bitcoin network). The public key, related and connected to the private key of the sender, is the key that allows crypto assets to be received by a certain address (receiver). The network, made of nodes,[69] validates every transaction which occurs in the given blockchain, matching the private key with the public key (linked to the private

69 Nodes are made of any kind of device with computational power (essentially computers or servers), each connected to other nodes; they constantly exchange the latest blockchain data. Basically, nodes store, spread and preserve the blockchain data, every node containing a full copy of the transaction history of the blockchain, which constitutes the infrastructure of a blockchain.

one).[70] The private key is kept secret, enabling the user to spend the crypto assets at a certain address. Put more simply, perhaps, the private key functions as a password, employed by the user to access its crypto assets. The public key, on the other hand, allows the nodes (being a peer-to-peer decentralised network) that verify the transaction to move the crypto assets from the sender address (authorised by the user employing its private key) to the receiver address.[71]

Users are also provided with wallets; these are a technical solution that allow users to manage together the crypto assets pertaining to different addresses. There are different types of wallets that may be provided to users. Essentially, these include i) online wallets, accessible online by users; ii) desktop wallets, which require the installation of software on a computer; iii) hardware wallets, consisting of two different types: paper wallets, which require the printing of the address and private key on a piece of paper, and wallets that require a computing device to work, since the crypto assets are kept inside the device.[72]

What is relevant for our purposes is the distinction between i) wallet service providers offering a custodian wallet service, and ii) wallet service providers that offer a non-custodial wallet. The fundamental difference lies in the fact that the former takes custody and control over the private keys of the user, while the latter does not. Among providers offering custodian wallet services, it is then possible to make a further distinction between a '*proper custodian*' and a '*full custodian*'. In the former, the wallet provider operates merely a custody service, only performing the orders made/given by users. In the latter, the wallet provider also gains access to the cryptocurrencies of users, administering such digital assets in the interest of the users.[73] Therefore, exchanges that offer custodian wallets may directly dispose of the users' cryptocurrencies.

---

70 For an in-depth discussion of how blockchain works, from a technical point of view, see Andreas M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Crypto-Currencies* (O'Reilly Media 2014).

71 Such a public-key encryption model, along with the use of the timestamp and the sequence of blocks, solves the issue of double-spending, removing the necessity of having an intermediary guarantee the transaction. See Nikolei Kaplanov, "Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation," (2012) 25 Loyola Consumer Law Review 111, 117–119. For a detailed and practical example of how a bitcoin transaction works, see Matthias Haentjens, de Graaf and Kokorin (n 66), 526–563.

72 We are talking about cryptocurrencies kept in 'cold' wallets, such as the Ledger wallet. Sometimes crypto assets are also subjected to exceptional security measures, and kept in a bunker; see Joon Ian Wong, "Switzerland's bitcoin bunker" (*Quartz*, 29 November 2017) <https://qz.com/email/quartz-obsession/1130471/>.

73 For a fully detailed description of different types of wallets and how they work, see Stefano Capaccioli, "Riflessioni sulla tassazione delle criptovalute: *wallet* quale deposito?," (2020) 6 L'Accertamento 62.

In the case of cryptocurrency custodian service providers, it is important to establish how to demonstrate ownership of the digital assets, as was done in the *Bitgrail* case. This is especially true when the exchange deposits the digital assets coming from users at addresses that commingle such assets (*omnibus* or pooled addresses), rather than keeping them stored at individual addresses for every user (segregated addresses). In the former hypothesis, probably easier from a technical and administrative point of view, disputes concerning ownership of a certain user over certain crypto assets may arise. That is because it is the crypto assets provider that maintains control over the private keys of these addresses, which makes it difficult to identify the property of a specific user.[74]

Such an issue could be resolved if custodian service providers were prevented from keeping users' funds together at an *omnibus* address. Indeed, if such digital assets were stored at segregated addresses, it would be possible to assert property rights over the digital assets deposited at such individual addresses. In addition, with the segregation model, the utilization of users' cryptocurrencies by the service provider is also prevented, both preserving client's funds in the event of insolvency and limiting the risk of losing cryptocurrencies in case of cyber-attacks (which happen regularly).[75]

This solution was recently suggested in the MiCA Proposal,[76] where the EU legislator provides, at Title V, a regulatory framework for crypto assets service providers. Starting from the definitions, the crypto assets services provided include "the custody and administration of crypto-assets on behalf of third parties,"[77] where "the custody and administration of crypto-assets on behalf of third parties means safekeeping or controlling, on behalf of third parties, crypto-assets or the means of access to such crypto-assets, where applicable in the form of private cryptographic keys."[78]

Article 63.1 of the MiCA Proposal states that:

> crypto-asset service providers that hold crypto-assets belonging to clients or the means of access to such crypto-assets shall make adequate

74 On this issue, for an in-depth analysis of the contractual relationship between users and exchanges, with the analysis of Gemini and Coinbase terms and conditions, see Matthias Haentjens, de Graaf and Kokorin (n 66).

75 In 2019, alone, 12 cryptocurrency exchanges have been hacked, resulting in losses of nearly $300M. For statistics and analysis of the individual cyber-attacks, see Selfkey, "A Comprehensive List of Cryptocurrency Exchange Hacks" (*Selfkey*, 13 February 2020) <https://selfkey.org/list-of-cryptocurrency-exchange-hacks/>.

76 MiCA Proposal (n 39), which we have analysed in Section 2.1 of this paper.

77 MiCA Proposal (n 39), Article 3, para. 9, subpara. a).

78 *Id*. at Article 3, para. 10.

> arrangements to safeguard the ownership rights of clients, especially in the event of the crypto-asset service provider's insolvency, and to prevent the [provider's] use of a client's crypto-assets on [its] own account except with the client's express consent.

It is indeed the express intention of the EU legislator to regulate the phenomenon we are dealing with, in order to preserve the property rights of clients over crypto assets in the event of insolvency. The definition contained in the regulation as "ownership rights" is a further indicator of the fact that digital assets should be treated as property.

With the aim of assuring the necessary separation of users' digital assets from those of the service providers, it is established that:

> crypto-asset service providers that are authorised for the custody and administration of crypto-assets on behalf of third parties shall segregate holdings on behalf of their clients from their own holdings. They shall ensure that, on the DLT, their clients' crypto-assets are held on separate addresses from those on which their own crypto-assets are held.[79]

The segregation of clients' crypto assets should, on the one hand, prevent the service provider from using such funds, thereby impeding the conclusion the court arrived at in the *Bitgrail* case. The *Bitgrail* court, indeed, rejected the restitution claim due to the fact that property over client's assets was acquired by the exchange as a consequence of the commingling of funds. On the other hand, keeping crypto assets at separate addresses should assure the preserving of property rights of users, since the link between clients and their crypto assets would always be traceable (and the transactions registered in the blockchain are public).

In addition to the issue of segregated addresses, it is also important to establish who maintains control over the private keys of the clients, in order to have the ability to dispose of such assets. In the event that the contractual relationship between parties establishes that private keys are to be kept and administered by the crypto assets service provider only, clients should demand the segregation of such assets, in order to avoid the digital assets falling within the insolvency estate, since the custodian has the power of direct disposal of the assets.

79 *Id*. at Article 67, para. 7.

Where, instead, the private keys are held jointly by the crypto assets custodian and the clients (but the custodian may not act without the user's consent), or by the clients only, there is no need to request segregation, since users will have the power to directly dispose of their digital assets, and so there would be no risk of commingling (if the said digital assets are kept at segregated, and not *omnibus*, addresses).

The MiCA Proposal does not seem to include a provision regarding the issue of segregation claims at the current stage.[80] This scenario is, instead, regulated by the Debt Enforcement and Bankruptcy Act of the Swiss federal government.[81] Article 242a provides that, where the crypto assets service providers have the keys to access clients' assets directly and the exclusive power to dispose of such assets, the clients have the right to ask for the segregation of their assets. Otherwise, in the absence of such power, the crypto assets would flow into the insolvency estate.[82]

As a consequence of the segregation of crypto assets, and the property rights over them, their owners could lodge a restitution claim in case of bankruptcy of the digital assets service provider and therefore ask for the return of the assets deposited. In such a hypothesis, investors would be able to get their digital assets back, if they prove ownership over them. Or at least this is what would happen in an ideal scenario, as in practice i) the investor must demonstrate ownership rights over specific digital assets; and ii) the insolvency trustee must recover such crypto assets from the bankrupt exchange, and give them back to the proprietor.

Otherwise, in the event their claims are deemed to be of a contractual/personal nature, the digital assets would be part of the insolvency estate, with the consequence of a *pari-passu* treatment of crypto-investors with other creditors in the proceedings. In this scenario, all the digital assets would be part of the insolvency estate, and clients would concur together, subject to payment

80 The MiCA Proposal only contains provisions directed at safekeeping digital assets and private keys, as laid down by Article 67, para. 3 of *id.*: "Crypto-asset service providers that are authorised for the custody and administration of crypto-assets on behalf of third parties shall establish a custody policy with internal rules and procedures to ensure the safekeeping or the control of such crypto-assets, or the means of access to the crypto-assets, such as cryptographic keys."

81 *Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register* vom 25. September 2020, BBI 2020 7801 (English: Act to Adapt Federal Law to Developments in Distributed Ledger Technology - DLT Act).

82 For a further examination of the Swiss draft law, see Benedikt Maurenbrecher and Urs Meier, "DLT Draft Law – Insolvency Law Aspects" (*CapLaw*, 31 March 2020) <https://caplaw.ch/2020/dlt-draft-law-insolvency-law-aspects/>.

priorities, with all other creditors of the bankrupted exchange (even those who have not invested in crypto assets), resulting in drastic reduction of the value of their claim.

4 Jurisdiction and Applicable Law in Insolvency Proceedings Regarding Cryptocurrencies: Private International Law Issues with Regard to Digital Assets

Crypto assets are built on the protocol that constitutes a blockchain. The blockchain is by definition decentralised, allowing parties to enter into a relationship without the intervention of an intermediary,[83] as it relies on a shared public ledger and a peer-to-peer technology. This centralisation poses some serious Private International Law (PIL) issues of jurisdiction and of applicable law. Indeed, this new disruptive technology is not easy to handle "through regulatory instruments designed for physical world objects, (state) territories and jurisdictions."[84]

That said, it is essential to establish which court is competent to open an insolvency proceeding, and which law is applicable to such proceeding; this will have important consequences for the treatment of the creditors and their claims against the bankrupt.

Crypto assets are not linked to any particular territory, which means that there is no obvious connection between a blockchain and any specific legal system. The traditional approaches to such PIL issues concerning insolvency (namely the universality and territoriality principles) do not work well when applied to crypto assets. For example, the (modified) universalist method[85] with the principle of COMI ("centre of main interest"),[86] adopted both by the European Insolvency Regulation[87] and the UNCITRAL Model Law,[88] does not

83 For the potential of the blockchain technology, see Vinay Gupta, "The Promise of Blockchain Is a World Without Middlemen" (*HBR*, 6 March 2017) <https://hbr.org/2017/03/the-promise-of-blockchain-is-a-world-without-middlemen>.

84 See Outi Korhonen and Jari Ala-Ruona, "Regulating the Blockchain Society," (2018) 3 Liikejuridiikka 77.

85 Providing that the insolvency proceeding will be opened in the state where the debtor has its domicile, and such law should govern all the assets pertaining to such debtor irrespective of where the relevant assets are located.

86 See in-depth discussion in the next paragraph.

87 Regulation (EU) 2015/848 of the European Parliament and of the Council of 20 May 2015 on insolvency proceedings, [2015] OJ L141/19 ("EIR Recast").

88 United Nations Commission on International Trade Law (UNCITRAL), "UNCITRAL Model Law on Cross-Border Insolvency with Guide to Enactment and Interpretation"

fit crypto assets. Indeed, such an approach focuses on the place which is the centre of the debtor's interests, a criterion which cannot be directly applied to blockchain, as the latter is decentralised by definition. Therefore, there is no 'centre of interest'; the transactions happening on a given blockchain are spread all around the nodes participating on the network, making it unviable to identify a physical place.

Such a statement is corroborated when dealing with decentralised autonomous organizations (DAOs), which are organizations run on the designed protocol, transparent, controlled by the members of the organizations and not influenced by a central authority, with the program rules and transactions/information registered on the blockchain. Thus, there is no central governance, no persons running the entity, and no physical properties. DAOs are essentially based on smart-contracts, which allow any participant from anywhere in the world to have an interaction with the organization like the one a person could have with an entity.[89] The COMI principle is therefore inapplicable to DAOs, as it is not possible to establish a main interest over an organization that is completely decentralised.

DAOs demonstrate how traditional PIL methods cannot be directly applied to blockchain, as the absence of any link with a state, any physical property or identifiable stakeholder, hamper the opening of an insolvency proceeding.[90]

The application of the *lex rei sitae* to Distributed Ledger Technology (DLT) also does not work well. This conflict-of-law rule establishes that rights on individual assets should be governed by the law of the place where such assets are located. Applying this criterion would lead to a substantially circular argument, since blockchain works on a distributed technology that has no link with any particular location. It could be argued that the location of crypto assets is that of the wallets; however, wallets are mere tools that enable users to access crypto assets, which are "located" on the distributed ledger. In addition, users could have multiple copies of a single wallet, making it impossible to determine which copy is relevant with regard to jurisdiction and applicable law. Crypto assets are built on a distributed ledger technology, meaning that they

---

(*UNCITRAL*, 2014) <https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/1997-model-law-insol-2013-guide-enactment-e.pdf> accessed 27 October 2022.

89 For additional information on how DAOs work, see Primavera De Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Harvard University Press 2018), 146–155.

90 See Ilya Kokorin, "The end of COMI as we know it: Insolvency rules in the era of decentralization," (Universiteit Leiden, 30 May 2017) <https://leidenlawblog.nl/articles/the-end-of-comi-as-we-know-it-insolvency-rules-in-the-era-of-decentralisati>.

are essentially in every single copy of a given blockchain, and therefore cannot be linked to any particular location.[91]

Blockchain therefore requires either an adaptation of the existing PIL connecting factors, or the creation of new ones, identifying new models that would work better with blockchain and its decentralisation. To this end, the Hague Conference on Private International Law *Conférence de La Haye de droit international privé* (HCCH) is tackling the issues arising from emerging technologies regarding jurisdiction and applicable law.[92]

Specifically, HCCH acknowledges that the traditional geographical locations related to PIL connecting factors is not relevant when speaking of DLT. It is thus necessary to develop different connecting factors, which may fit better with blockchain.[93] HCCH is considering the possibility of adopting criteria that do not take into account the place where the asset is located or the place where the transaction was made, but rather the place where the participant, or the relevant authority, is located.

What is more, new connecting factors have been envisaged by HCCH in order to better encompass digital assets, involving the application of IT criteria. For example, HCCH makes reference to the '*lex codicis*' or '*lex digitalis*', which considers the governing law to be that of the code that was used to create the relevant IT program.[94] *Lex digitalis* would imply that the applicable law be linked to the governing law of the code used to write the original distributed ledger program, choosing different factors, such as the place of the residence of the coder. That solution is not completely convincing, for multiple reasons, for example: i) the coder could be anonymous, or use a pseudonym, therefore making that criterion uncertain; and ii) blockchain is decentralised, so there is no central administrator, and the coder could, as was the case with Satoshi Nakamoto regarding Bitcoin, disappear, and not participate in the further development of the network. Thus, linking the applicable law to the mere creator of the code does not appear to be an appropriate solution.

---

91 See INSOL International (n 57), 34–36, where the authors discuss the difficulties in finding an appropriate solution to the application of *lex rei sitae* criterion to digital assets.

92 Hague Conference on Private International Law (HCCH), "Developments with Respect to PIL Implications of the Digital Economy, Including DLT: Prel. Doc. No 4 of November 2020" (*HCCH*, March 2021) <https://assets.hcch.net/docs/8bdc7071-c324-4660-96bc-86efba6214f2.pdf> accessed 27 October 2022.

93 *Id*. at para. 16–18. HCCH pointed out that a significant difference may be drawn between "permissioned" and "permissionless" blockchains. In the former, participants in the network must be admitted, thereby becoming identifiable. In the latter, on the contrary, users may participate without any authorisation.

94 For a full list of new connecting factors based on modern technologies, see *id*. at Annex I.

Given the difficulties of finding a feasible solution to the jurisdiction and applicable law issues, the *lex digitalis* was also advocated as a modern approach of the theory known as "contractualism."[95] In particular, the *lex digitalis* would be useful in the case of DAOs organization, giving a practical approach to solve the issues posed by the cross-border environments in which these organizations operate.[96] Indeed, the choice of jurisdiction and governing law in the form of the code would provide some legal certainty and predictability to the investors, otherwise being subject to less predictability when trying to ascertain the applicable law and jurisdiction.

5 Competent Court and Applicable Law in Case of Insolvency of Crypto-Assets Service Providers

In contrast to the case of crypto asset owners, the universality approach and COMI continue to be valid when speaking of the insolvency of crypto asset service providers (exchange and third-party wallet providers), since they are entities registered in a specific State.

The main benefit of the COMI principle is that of legal certainty, since insolvency proceedings are treated in a predictable and efficient way. In addition, COMI prevents the opening of parallel insolvency proceedings, merging the creditors' claims into only one procedure, to the benefit of the creditors as a reduction of transaction costs, and also of the debtor's estate, avoiding a piecemeal sale of such assets.[97]

We have already mentioned that the principle of modified universalism is applied in the EU regulatory framework. Transnational insolvency between Member States (with the exclusion of Denmark) is indeed regulated by the Regulation (EU) 2015/848 of the European Parliament and of the Council of 20 May 2015 on insolvency proceedings (also known as EIR Recast).[98] Among the objectives pursued by the EU legislator was "the proper functioning of the

95 According to Robert K. Rasmussen, "A New Approach to Transnational Insolvencies," (1997) 19 Michigan Journal of International Law 1, companies should have in their corporate charters the election for the jurisdiction applicable in case of insolvency.

96 See Kokorin (n 90).

97 *Id.*

98 Insurance undertakings, credit institutions, investment firms and other firms, institutions or undertakings covered by Directive 2001/24/EC of the European Parliament and of the Council of 4 April 2001 on the reorganisation and winding up of credit institutions, [2001] OJ L125/5 and collective investment undertakings are excluded from the application of EIR recast (n 87), as laid down under Recital no. 19.

internal market [which] requires that cross-border insolvency proceedings should operate efficiently and effectively."[99] To that end, it is provided that the EIR Recast aims to "avoid incentives for parties to transfer assets or judicial proceedings from one Member State to another, seeking to obtain a more favourable legal position to the detriment of the general body of creditors (forum shopping)."[100]

According to the EIR Recast: i) the courts of the Member State within the territory of which is situated the centre of the debtor's main interests (COMI) shall have jurisdiction to open insolvency proceedings; ii) courts of such Member State are competent to seize all of the debtor's assets, regardless of their location;[101] iii) when an insolvency proceeding is opened in a Member State, the courts of another Member State shall have jurisdiction to open a secondary insolvency proceedings against that debtor only if the debtor possesses an establishment within the territory of that other Member State, which will be limited to the assets localised in that State.[102]

The main bankruptcy proceeding is thus opened in the Member State where the debtor has his/her COMI. The regulation specifies that "the centre of main interests shall be the place where the debtor conducts the administration of its interests on a regular basis and which is ascertainable by third parties."[103] The same article then imposes a series of presumptions concerning the place of COMI for legal persons, individuals exercising a professional activity and other individuals. For the purposes of this paper and regarding the insolvency of crypto asset service providers, the place of the registered office shall be presumed to be the centre of its main interests in the absence of proof to the contrary.[104]

In addition to the regulation of jurisdiction, the principle of COMI also governs the law applicable to the bankruptcy proceedings, since Article 7 of EIR Recast establishes that the law applicable to insolvency proceedings and their effects shall be that of the Member State within the territory of which such proceedings are opened, with the exceptions laid down in that regulation.

The COMI principle laid down by EIR Recast is deemed to be a proper criterion to establish jurisdiction and applicable law, since it enables the Member State that has been affected the most by the bankruptcy to open and govern

99 EIR Recast (n 87), Recital no. 3.
100 *Id.* at Recital no. 5.
101 *Id.* at Recital no. 23.
102 *Id.* at Recital no 23 and Article no. 3.
103 *Id.*
104 *Id.*

the insolvency proceeding.[105] The certainty and predictability of the COMI is extremely relevant to bankruptcy proceedings, as, by being able to predetermine the competent court and the applicable law, it makes possible an *a priori* assessment of the outcomes of the insolvency proceedings.[106]

With regard to the insolvency of crypto asset service providers, it is at this point necessary to combine the regulatory framework laid down in the EIR Recast with that contained in the recent MiCA Proposal. Article 53(1) of the latter provides that crypto assets services shall only be provided by legal persons that have a registered office in a Member State of the European Union and that have been authorised as crypto asset service providers. The application for such authorisation is made to the competent authority of the Member State where the crypto asset service provider has its registered office (article 54(1). Based on those rules, insolvency proceedings concerning crypto asset service providers are opened in the Member State where the providers have their registered office (COMI presumption).

With regard to jurisdiction, there should be the same treatment of creditors' claims independently from the qualification of such claims as credit or proprietary. Indeed, Article 6.1 of EIR Recast recognises the principle of *vis attractiva*, stating that:

> the courts of the Member State within the territory of which insolvency proceedings have been opened in accordance with Article 3 shall have jurisdiction for any action which derives directly from the insolvency proceedings and is closely linked with them.

Such rule posits that claims of investors against a crypto asset service provider, as they derive from insolvency proceedings and are linked to them, would be subject to the COMI principle with regard to jurisdiction. Here, the characterisation of the investors' claims is not relevant, as they are still subject to the *vis attractiva* rule laid down in provision of Article 6(1) of EIR Recast.

However, the possibility of characterising some crypto assets as property leads to different treatment with regard to the law applicable to

105 See Federico M. Mucciarelli, "Private International Law Rules in the Insolvency Regulation Recast: A Reform or a Restatement of the Status Quo?" (*SSRN*, 25 August 2015) <https://ssrn.com/abstract=2650414>.

106 For a deeper analysis on the EIR recast and the principle of COMI, see Francisco Garcimartín, "The EU Insolvency Regulation Recast: Scope and Rules on Jurisdiction" (*SSRN*, 24 March 2016) <https://ssrn.com/abstract=2752412>; Dario Latella, "The 'COMI' Concept in the Revision of the European Insolvency Regulation" (*SSRN*, 27 September 2013) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2336470>.

crypto-investors' claims, as different conflict-of-law rules apply to crypto assets investors' claims depending on whether they are deemed to be of a personal or proprietary nature.

If we assume that investors' rights are qualified as rights of claims, such claims would be subject to the *lex fori*, such that the applicable law would be that of the place where the insolvency proceedings were opened. By contrast, different conflict-of-law rules apply to claims having a proprietary nature. In fact, Article 8 of EIR Recast contains an exception to the *lex fori* principle with regard to the rights *in rem* of creditors or third parties. The first paragraph of this article establishes that:

> the opening of insolvency proceedings shall not affect the rights *in rem* of creditors or third parties in respect of tangible or intangible, moveable or immoveable assets, both specific assets and collections of indefinite assets as a whole which change from time to time, belonging to the debtor which are situated within the territory of another Member State at the time of the opening of proceedings.

Among the actions explicitly excluded from the application of the *vis attractiva* principle (*i.e.* the law of the Member State in which the proceeding is held), there are "the right to demand assets from, and/or to require restitution by, anyone having possession or use of them contrary to the wishes of the party so entitled," as set forth under Article 8(2)(c), of EIR Recast.

On this issue, the ECJ confirmed that restitution claims are independent from the insolvency proceedings, as it expressly stated that restitution "constitutes an independent claim, as it is not based on the law of the insolvency proceedings and requires neither the opening of such proceedings nor the involvement of a liquidator."[107]

Thus, the qualification of digital assets such as cryptocurrencies as property would imply considering creditors' claims as proprietary in nature;[108] such actions would then fall under the provision of Article 8(2)(c), as they would be included among "the right to demand assets from, and/or to require restitution." Owners of digital assets would then be able to lodge a claim for the restitution of their crypto-properties without being subject to the insolvency proceedings and its rules, because such a claim would be an independent one and would not fall under the law of the insolvency proceedings.

---

107 *German Graphics Graphische Maschinen GmbH v Alice van der Schee*, ECJ Case C-292/08, Judgment of the Court (First Chamber) of 10 September 2009, ECLI:EU:C:2009:544.

108 For an in-depth analysis of the topic, see Matthias Haentjens, de Graaf and Kokorin, (n 66).

With reference to the law applicable to crypto assets claims of a proprietary nature, at this stage, there is still no unanimously approved solution, since, as noted in the previous paragraph, the issue of finding connecting factors that would fit the blockchain is still subject to debate. In the EU legal framework, reference should be made to Article 67(1)(f) of the recent MiCA Proposal, which provides that the agreement between crypto asset service providers authorised for the custody and administration on behalf of third parties and clients should include the reference to the law applicable to that agreement. It is thus a contractual choice of law applicable to the agreement, stipulated by the parties. Given that claims of a proprietary nature are not included in the *vis attractiva* of the debtor's COMI, establishing the law applicable to such claims in advance may provide some legal certainty to crypto-investors, and a reduction of the transaction costs that would arise if there were no predetermination of the law applicable to such claims.

Therefore, the treatment of creditors of an insolvent crypto asset service provider is strongly influenced by the legal qualification of the nature of the creditors' claim. In the event that creditors are deemed to have a personal claim, it will follow that they will be creditors of the bankruptcy estate (which also includes the digital assets they deposited) for a credit right corresponding to the monetary value of their asset, subject to the bankruptcy reduction and to competition with other unsecured debt (with satisfaction depending on the payment priorities). Regarding jurisdiction and applicable law, in this case, their actions would be affected by the *vis attractiva* of the insolvency proceedings, and be fully subject to the provisions laid down under EIR Recast. As a consequence, crypto asset service providers' clients must lodge their claims (credit) in the Member State where the insolvency proceeding was opened, and the law of that State will apply.

Conversely, should it be determined that the action is proprietary in nature, then the creditors will be able to claim the return of the crypto assets deposited, directly claiming the restitution of the digital assets they own. In this case, they will not compete with the other creditors of the bankruptcy, and will be entitled to full restitution (in the ideal case where the insolvency trustee manages to get access to the crypto asset service provider's assets, given the technological challenges raised by blockchain). With regard to jurisdiction over such a claim, since it derives from and is linked to the insolvency proceeding, it is subject to the COMI principle established in the EIR Recast, and therefore will lie with the Member State where the bankruptcy proceeding was opened. On the other hand, there are greater uncertainties concerning the law applicable to claims qualified as being of a proprietary nature. On this point, the most

feasible solution appears to be that offered by Article 67(1)(f) of the recent MiCA Proposal, giving the parties the possibility of choosing the applicable law.

In summary, then, the various types of crypto assets demand particular attention before investing, since the buyer must evaluate carefully the legal nature of such assets (activity facilitated by the publication of the white paper by the issuer, as imposed by the MiCA Proposal for certain crypto assets), as such nature has a significant impact on regulation and protection in the event of the insolvency of the providers. Indeed, certain crypto assets, such as electronic money tokens, that give a right to claim against the crypto asset service provider as laid down in Article 44 of the MiCA Proposal, allow the investor to simply make a personal claim. As a consequence, such claims will be subject to payment priorities along with the other creditors of the provider, as well as to the COMI principle and to the *lex fori* with regard to jurisdiction and applicable law. In contrast, however, given that "the crypto-assets are automatically created through mining as a reward for the maintenance of the DLT or the validation of transactions" as provided by Article 4(2)(b) of the MiCA Proposal, should be considered properties. Such a qualification has different benefits in the context of insolvency proceedings of crypto-asset service providers. First of all, cryptocurrency investors have a right to ask for the restitution of their assets and not merely a right to make a claim. In addition, while jurisdiction would be subject to the COMI principle, the parties could choose the applicable law in the contract, as laid down in the MiCA Proposal, resulting in more legal certainty, to the benefit of investors and of the legal system in general.

CHAPTER 16

The Law Governing Secured Transactions in Digital Assets

Matthias Haentjens and Matthias Lehmann

1 Introduction: Practical Relevance and Legal Problems of Secured Transactions in Digital Assets*

Despite their relatively recent emergence, and despite the fact that many of them do not represent any "real world" asset, digital assets – such as cryptocurrencies or tokens – are becoming both increasingly valuable and increasingly common. This makes them interesting also as an object for secured transactions, which could raise (additional) value for the holder of such assets. After all, why leave your bitcoin sitting idly on a USB key, when it could be used as collateral for a loan or other financial transactions?

The use of digital assets as collateral is especially relevant in light of the current scarcity of other assets that can be used as collateral, whether financial or non-financial. This scarcity is due to a number of different causes. Foremost among them are the COVID-19 pandemic and more recently the war in Ukraine, which have caused an economic slowdown; have limited the circulation of money, securities as well as commodities; and, have destroyed valuable assets. Central banks upped the ante by throwing cash into the financial markets – partly in a reaction to the pandemic – , with the consequential spiralling of asset prices. In addition, regulatory developments have contributed to the 'collateral crunch', such as the stricter capital requirements for banks under the latest Basel regime and the mandatory central clearing requirement for important categories of derivatives, which all require additional collateral.

Digital assets may at least partly cover this shortfall as it may be argued that they are particularly well suited to serve as collateral in secured transactions. This has to do with some of their properties: first, the technological infrastructure for digital assets, *i.e.* Distributed Ledger Technology (DLT) or blockchain has been specifically designed to minimise the risk of fraud, as DLT aims to avoid double spending by making transactions irreversible through the combined use of a network validation mechanism and cryptographic methods,

* Many thanks to Emeric Prévost for his help and useful comments on the manuscript.

© MATTHIAS HAENTJENS AND MATTHIAS LEHMANN, 2023 | DOI:10.1163/9789004514850_018
This is an open access chapter distributed under the terms of the CC BY-NC-ND 4.0 license.

which create an immutable record.[1] Second, the transfer of digital assets is relatively straightforward; as a matter of fact, Bitcoin – the first fully decentralised blockchain – was conceived as a global peer-to-peer transfer mechanism on which value was supposed to be transferred from one party to another without the need for any intermediary. Third, the value of most digital assets can be easily determined as the current price is published regularly, similarly to share or bond prices, in various media and can be gleaned from offers by crypto exchanges. Since the euphoria of the first years, all three properties just discussed must be nuanced: first, over the last years, several digital assets, networks, and crypto-exchanges have been the victims of serious hacks which cost investors a fortune; second, a transfer of bitcoins nowadays takes a long time to settle because validation on the blockchain has become increasingly difficult and expensive, which is one of the reasons why most investors now use intermediaries such as crypto-exchanges and wallet providers to transfer their digital assets; and third, the value of most digital assets has proven to be extremely volatile. Nonetheless, digital assets are still considered to be well suited to serve as collateral in secured transactions, especially because of their spectacular growth.

Consequently, it is anything but surprising that the interest in transactions secured by digital assets has soared. A striking example is provided by the first Bitcoin-backed loan, which was recently offered for the first time in history.[2] Goldman Sachs granted opened a lending facility in fiat currency for the borrower, who secured it with Bitcoin as collateral. The bank stated that it was particularly attracted by the opportunity for 24-7-365 day risk management.[3] The same possibility was also raised in the debate about crypto derivatives clearing and settlement, which was ignited by FTX-owner and billionaire Sam Bankman-Fried.[4] One of the main arguments for such a revolutionary approach to derivatives clearing and settlement is the possibility of managing collateral in real time.[5]

---

1 See Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (*Bitcoin*) <https://bitcoin.org/bitcoin.pdf> accessed 26 May 2022.

2 Shashank Bhardwaj, "Goldman Sachs rolls out first bitcoin-backed loan" (*Forbes*) <https://www.forbesindia.com/article/crypto-made-easy/goldman-sachs-rolls-out-first-bitcoin backed-loan/75833/1> accessed 31 May 2022.

3 *Id.*

4 Javier Paz, "FTX CEO Sam Bankman-Fried To Defend His Disruptive Plan For Crypto Derivatives In Front Of Congress" (*Forbes*, 12 May 2022) <https://www.forbes.com/sites/javierpaz/2022/05/12/ftx-ceo-sam-bankman-fried-to-defend-his-disruptive-plan-for-crypto-derivatives-in-front-of-congress/?sh=78b88e9c42a6>.

5 *Id.*

A further illustration is a complex project dubbed "Security Tokens Refinancing" carried out by the company *Forges*, a subsidiary of the French bank *Société Générale*.[6] According to media reports, the company plans to issue "security tokens" backed by mortgages to the tune of US$ 40 million, which will be used as collateral for a loan of the stablecoin DAI worth US$ 20 million. The lender here will not be a traditional financial intermediary, but MakerDAO, the decentralised finance (defi) protocol. Importantly for present purposes, the "security tokens" will be deposited with a security agent. The structure of the operation is quite complex and involves in total no less than six entities.

There are also very simple forms of collateral arrangements. A most basic version is described in Satoshi Nakamoto's initial white paper itself: when discussing sales transactions, he contends that "routine escrow mechanisms could easily be implemented to protect buyers," after having hailed the virtues of bitcoin transfers for sellers.[7] This would mean holding back or reserving title in the bitcoins sold until the seller's performance. The fact that Nakamoto uses a legal term ("escrow") is quite revealing because it demonstrates the continuing importance of the law even in the highly technological context of Bitcoin, which is normally a no-go for crypto aficionados. Although legally to be distinguished from the creation of a security rights in certain assets, reservation of title and escrow accounts are time-honoured methods of securing the performance of a debtor.

Since Nakamoto's white paper, secured transactions have taken on a wholly different function in the context of new and innovative operations on the blockchain. A first example of this is "staking." Staking plays an important role in "proof of stake" mechanisms, which increasingly replace "proof of work" mechanisms. Both serve to shield the verification of blocks, or mining, against the risk of manipulations by a malevolent node, *i.e.* an ill-intentioned participant in the blockchain. As is well-known, "proof of work" mechanisms means that mining nodes compete against each other until one miner or mining pool comes out as the first to solve the "hashing" algorithmic riddle[8] that allows for the addition of a new block of transactions to the chain; since this requires considerable computing power and energy, it would be too cumbersome to do this effort for a malevolent node on a large scale. The proof of work mechanism

6 See Florent D, "La Société Générale fait une proposition à MakerDAO" (*Cryptoast*, 2 October 2021) <https://cryptoast.fr/societe-generale-collaboration-historique-defi-makerdao/>.

7 Nakamoto (n 1), 1.

8 Simply put, "hashing" refers to the algorithmic process of randomly converting an arbitrary amount of data bytes input into a fixed amount of encrypted data output (generally represented on a hexadecimal (hex) base). For instance, Bitcoin uses the SHA-256 hash algorithm.

has fallen out of favour, though, because of its high-energy consumption. In proof of stake mechanisms, it is no longer necessary to solve a mathematical riddle in the validation/mining process, but nodes evidence their serious intentions by the stake they have in the network, in particular through the digital assets they own. To acquire more of these assets, and to be able to do more mining, some nodes simply offer other users a participation in the profits they make from using their digital assets. Staking thus means the use of one's assets for this purpose. In this process, the relevant assets will be blocked, frozen, or locked up, depending on the particular network. It does not seem far-fetched to compare the operation of staking with placing assets in escrow to secure the performance of an obligation, and therefore with a secured transaction, the conditions of which vary with the network in question.

Another example of an innovative blockchain operation in which secured transactions may play a role is "yield farming." This operation is relevant in the context of Decentralised Finance, or "DeFi." It consists in the lending of digital assets to a DeFi platform, *e.g.*, a decentralised exchange (Dex), which will use it as liquidity for its pool. The lender receives in return a portion of the platform's fees and return. Yield farming may involve an outright transfer, with a later right of return, similar to a repurchase (repo) transaction. But where the digital assets are merely locked up or "bonded," it may as well be assimilated to a secured transaction: the platform acquires a secured right in customer's asset(s).

Because of the operations just explained, but also because of the current scarcity of other categories of assets that can be used as financial collateral as discussed earlier, it is to be expected that the use of digital assets as collateral is going to rise in the years to come. This raises a number of legal questions. Among the most salient is that of the applicable law: which legal system governs a secured transaction in digital assets? And, more precisely: which law determines the requirements for the validity and the effects of security rights in digital assets?

The need to answer those questions cannot be negated by the slogan "code is law." This slogan was originally coined by Lawrence Lessig to demonstrate the need to regulate the internet,[9] but is often abused for precisely the opposite purpose, *viz.* for denying the need for law and legal regulation of the internet in general and of the blockchain in particular. Notwithstanding the claims

9 Lawrence Lessig, "Code Is Law" (*Harvard Magazine*, 1 January 2000) <https://www.harvardmagazine.com/2000/01/code-is-law-html> accessed 20 March 2022; see also Lawrence Lessig, *Code: And Other Laws of Cyberspace, Version 2.0* (2nd edn, Basic Books 2006).

of some radical believers in the autonomy of the blockchain, digital assets are and will always be subject to the law and legal rules. Moreover, digital assets need law.

First, there are legal constructs and mechanisms that even the most autonomous DLT cannot code around. For instance, when the world's then leading bitcoin exchange Mount Gox was declared bankrupt in 2014, no code could have prevented the Tokyo District Court to assert jurisdiction and decide how the digital assets and their proceeds connected with the exchange should be distributed amongst creditors.

Moreover, even the staunchest believers in DLT and blockchain claim that investors in digital assets have "ownership" of those assets. Nakamoto, in his 9-page white paper, for instance, uses "own" and "ownership" of bitcoin and its keys 25 times. Ownership is a legal term deeply rooted in history which is, has been, and will be used to protect those who claim entitlement to assets. Therefore, digital assets also need (the application of) this doctrine. More generally, and as a matter of principle, digital assets need the application of proprietary rights, which are generally believed to provide certainty and predictability because they have effects against everybody, or *erga omnes*.

Law and legal rules more or less rigidly regulate proprietary rights, precisely because of their *erga omnes* effects. One of the first questions that the court had to decide when Mount Gox was declared insolvent, for instance, was whether the investors had proprietary rights in the digital assets under Japanese law, a question that was ultimately denied by the Tokyo District Court.[10]

The need for law and legal rules is even stronger with regard to security rights as a sub-set of proprietary rights. The *raison d'être* of security rights is to secure the position of the creditor and minimise its counterparty risk; a security right that would not provide certainty and predictability of protection against the debtor and its other creditors would be futile. While it is true that technology can factually provide the creditor with the possibility to dispose of an asset or block transfers that would endanger his rights, this is not always sufficient to safeguard his position. For instance, the need for legal help arises where the blockchain is hacked and the assets that serve as collateral have been stolen. Similarly, other creditors, with equally or stronger technological capabilities,

10 Tokyo District Court, Reference number 25541521, Case claiming the bitcoin transfer, etc., Heisei 26 (Year of 2014), (Wa) 33320, Judgment of Civil Division 28 of 5th August 2015; English translation by Megumi Hara, Charles Mooney and Louise Gullifer, available at <https://www.law.ox.ac.uk/sites/files/oxlaw/mtgox_judgment_final.pdf> accessed 26 May 2022.

may compete for the same asset. Thus, (also) digital assets need law to prevent the technologically strongest from prevailing.

In the following, we will first examine whether the law governing the requirements for the validity and effects of security rights in digital assets deserves a specific rule, or whether the same rule can be used as that which determines the law governing the relevant network (2). As a matter of principle, we believe the first assertion is correct, save for exceptional cases, such as a permissioned blockchain operated and/or supervised in a specific country only. Therefore, we will argue which law should govern security rights in digital assets independently. To do so, we draw a distinction between digital assets that are "held" by a (crypto-) custodian and those that are not. We first analyse which law should apply to digital assets that are "held" by a (crypto-) custodian (3). For digital assets that are not so "held," we determine whether security rights in digital assets can be subject to a choice of law, *i.e.* to the principle party autonomy (4.1). After that, we argue which law should apply to these digital assets in the absence of a choice (4.2). Because of the universal nature and world-wide accessibility of digital assets recorded on a blockchain, the issue of "control" plays a special role. This raises the question as to whether such control should be defined in a globally uniform way, independently of the governing law (5). Finally, we deal with the law governing remaining legal issues, such as capacity, error, fraud, succession or insolvency, which will be summarised under the catchphrase "other laws" (6).

Though our study is quite extensive, we do not strive to be comprehensive. Therefore, we will not cover all issues connected with secured transactions on the blockchain. Specifically, we will not deal with the question of which court may or should have jurisdiction with regard to disputes that may arise out of such transactions. We also do not address specific insolvency law issues, such as fraudulent transfers (of digital assets). This does not exclude that our analysis will be most helpful in the case of insolvency proceedings when the law applicable to a secured transaction needs to be determined, because such analysis has to be made independently of the law governing the insolvency, or *lex fori concursus*.[11]

Finally, whilst we do cover proprietary rights in digital assets, we do not intend to do so exhaustively. This chapter is limited to the extent that, first, we will focus on Private International Law (PIL) rather than substantive law (although matters of substantive law will be covered in section 5), and, second, we will specifically investigate the law that should apply to security rights in

11 See, *e.g.*, Regulation (EU) 2015/848 of the European Parliament and of the Council of 20 May 2015 on insolvency proceedings, [2015] OJ L 141/19 ("EU Insolvency Regulation").

digital assets. Therefore, we will not extensively discuss the law applicable to ownership. On the other hand, we do understand "secured transactions" in a broad sense, such that we intend to cover both transactions in which security rights *stricto sensu* (such as pledges, liens, hypothecs, *etc.*) are created in digital assets for the benefit of a creditor, and transactions in which (full) ownership in digital assets is transferred to a creditor for the purpose of securing a debtor's obligation(s). These latter transactions are sometimes referred to as "title transfer collateral arrangements,"[12] and are within the remit of our investigation.

2 The Independence of the Law Governing the Secured Transaction from the Law Governing the Blockchain

It is well known that the law applicable to the blockchain, as such, or to assets recorded on the blockchain, poses difficult questions of conflict of laws.[13] The blockchain is a decentralised network with nodes dispersed all over the planet. This makes it nearly impossible to localise it or otherwise find a closest or most significant connection with a single state or jurisdiction. It also seems undesirable that the law of one state, say New York law or England, should govern the entire blockchain and all the operations happening in connection with it. In sum, it does not promise much success to try to connect an inherently global and virtual phenomenon to a specific, physical, and geographically localised asset.

At this point, it is unnecessary to restate the discussion of this conundrum and the solutions that have been suggested to resolve it. Fortunately, our task is somewhat easier: we do not need to localise the blockchain as such or determine the specific asset recorded on it. Instead, we must "only" determine the law that applies to a secured transaction and to security rights vested in digital assets. This law could be the same as that governing the network and the assets recorded thereon. However, we would argue that as a matter of principle, the law governing a secured transaction and security rights vested in digital assets may be different from that governing the blockchain and the assets as such.

12 See, *e.g.*, Directive 2002/47/EC of the European Parliament and of the Council of 6 June 2002 on financial collateral arrangements [2002] OJ L 168/43, Art. 2(1)(b) ("Financial Collateral Directive").

13 See the other contributions in this volume.

Such an "independence" is not new or unheard of. In reality, it has long been recognised for other assets. One case in point is that of claims or receivables: Under the UNCITRAL Convention on this topic, their assignment may be governed by a law different than that governing the original contract by which the receivable was created.[14] The UNCITRAL Model Law on Secured Transactions suggests more generally for the security right in *any* intangible asset that the law applicable is the law of the place of residence of the provider of such security.[15] Both of these international texts thus assume that the law governing a security right is independent from the law governing the asset as such.

This "principle of independence" is not absolute and does not need to apply to blockchains that are exclusively governed by the law of a specific country. The paradigm case here is a network the nodes of which are all located in the same country: in this case, it is obvious that the only connection is with this country. An example that is more likely to occur in practice is a permissioned network where a central operator is located in a specific country.[16] Networks regulated and supervised by the financial authorities of only one state are another illustration[17] wherein the closest connection of the whole network will obviously be with that state. It thus stands to reason to consider

14 United Nations, *United Nations Convention on the Assignment of Receivables in International Trade* (New York: United Nations Publications, 2004), Art. 30 (submitting the priority of the right of an assignee to the law of the state in which the assignor is located). On this provision, see also *infra* section IV(2).

15 UNCITRAL, "Model Law on Secured Transactions" (*United Nations*, 16 February 2017), Art. 86 <https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/19-08779_e_ebook.pdf> (submitting the creation, effectiveness against third parties and priority of a security right in an intangible asset to the law of the State in which the grantor is located). On this provision, see also *infra* section IV(2).

16 For instance, one could think of a blockchain between multiple banks and other financial service providers that is run by one of them.

17 See the "crypto securities register" (*Kryptowertpapierregister*) in German law, which are supervised by the German BaFin, BaFin "Kryptowertpapierliste nach eWpG" (*BaFin*, updated 24 May 2022) <https://www.bafin.de/DE/PublikationenDaten/Datenbanken/Kryptowertpapiere/kryptowertpapiere_artikel.html?nn=7845918>; see Das Gesetz zur Einführung von elektronischen Wertpapieren vom 3. Juni 2021 (BGBI. I S. 1423), sec. 11. See also the Federal Act on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading (Financial Market Infrastructure Act, FinMIA) of 19 June 2015, RS 958.1, Art 73a et seq. (requiring the operators of "DLT trading systems" (*DLT Handelssysteme*) to be registered with the Swiss FINMA).

the law of this state as governing any secured transaction with regard to assets recorded on that network.[18]

The independence of the law governing the blockchain from the secured transaction is however of vital interest in the case of permissionless blockchains, where the law applicable to the blockchain itself is notoriously difficult to determine. In fact, such an independence may more often than not be the *only* chance to determine the applicable law in a legally certain way *at all*. An example is the Bitcoin blockchain, where a law governing the whole blockchain is not identifiable.

On the other hand, the independence principle is also not without issues. First, it may result in a different law applying to the security right and the encumbered digital asset, which may be problematic *per se*. For instance, the law applying to the creation of the security right may require that for a valid creation of a security right such as a pledge, the pledgee must be the owner of the (digital) asset. Typically, however, ownership is to be determined by the law that applies to the asset itself, which may thus be a different law. Also, the law applying to the security right may not be easily foreseeable to third parties, which can be considered as problematic because security rights, as a sub-set of proprietary rights, apply *erga omnes*. Finally, the independent determination of the law governing security rights in digital assets may lead to conflicting laws following from various secured transactions related to the same digital asset, without a 'meta'-law that determines the priority between those laws. These problems are not without solutions, but they depend on the specific conflict-of-laws rule chosen to govern security rights in digital assets, and will therefore be discussed in their context below.

In sum, where it is clear that a network is governed by the law of a particular state, this law should also apply to secured transactions and the security rights vested in digital assets recorded on that network. By contrast, the following analysis will focus on situations in which a law governing the whole network is *not* clearly submitted to one law exclusively. It is only then that the law governing the secured transaction and the security rights vested in digital assets must separately be determined.

18 Explicitly in this sense; see the German Act on the Introduction of Electronic Securities of 3 June 2021 (*Gesetz zur Einführung von elektronischen Wertpapieren*) (Federal Law Gazette I p. 1423), sec. 32.

3 Digital Assets "Held" by a Custodian

As already stated above, the blockchain was originally conceived as a mechanism for the direct, or "peer-to-peer," transfer of digital assets, but most of these assets are today held through a service provider, such as a crypto-exchange or a wallet provider. For our present purposes, we call both types of service provider, perhaps somewhat counterintuitively, a "custodian." In our view, where digital assets are "held" by a custodian, this custodian forms an indispensable link between the investor and their assets because the investor cannot dispose of its assets without the custodian's cooperation. For the purposes of determining the law that applies to the investor's proprietary rights in his digital assets, the custodian therefore forms the closest connecting factor.[19] In other words, the investor-custodian relationship must determine the law that governs the investor's proprietary rights in the digital assets in custody, because the custodian exercises factual control over those assets. Control corresponds to possession in the real world. In other words, in more than a merely metaphorical way it could be said that rights in digital assets are "located" with the custodian. Connecting the law governing an investor's proprietary rights in his digital assets to the custodian also has another advantage: it allows the investor to dispose of its entire portfolio of digital assets held with the same custodian under the same law. Otherwise, the investor and custodian may have to comply with the rules of multiple laws to transfer, or create security rights in the same digital assets portfolio. To have one law govern the entire portfolio would therefore considerably facilitate the lives of both the investor and its custodian, as the experience with intermediated securities has also demonstrated.[20]

The law of the investor-custodian relationship should thus determine the validity and effects of security rights in digital assets held through a custodian. This is true both for the situation in which the custodian itself is the security taker, and for the situation in which the security taker is a third party, such as the investor's creditor or a DeFi-Platform. In both cases, the validity and effects of security rights in digital assets should be subject to the "custody law."

Which law is this custody law that should apply to secured transactions? In this regard, the 2006 Hague Convention on Intermediated Securities

19 Matthias Haentjens, Tycho de Graaf and Ilya Kokorin, "The Failed Hopes of Disintermediation: Crypto-Custodian Insolvency, Legal Risks and How to Avoid Them" (2020) 2 Singapore Journal of Legal Studies 526, 526–563.

20 See, on the law applicable to intermediated securities, *e.g.*, Matthias Haentjens, *Harmonisation of Securities Law: Custody and Transfer of Securities in European Private Law Private Law* (Alphen aan den Rijn: Kluwer Law International 2007), 36–40 and the references there given.

(hereinafter, the "Hague Securities Convention")[21] is instructive. The Convention deals with securities that are held by an intermediary for a client. In practice, the vast majority of securities is uncertificated and exists only as a book-entry into a securities account, *i.e.* an electronic record. The custody of intermediated or book-entry securities is thus not entirely dissimilar to the custody of digital assets.

The Hague Securities Convention says how to determine the law of custody for intermediated securities. In its Article 4, the principle of party autonomy takes centre stage, which means that client and custodian are free to choose the law governing the proprietary rights in the securities held by the intermediary. If they have not specifically chosen a law to govern proprietary rights, these rights are governed by the law they have chosen to govern the agreement between the custodian and the client.[22] Given the similarity of the custody of book-entry securities and of digital assets, it makes sense to follow the same principle in the blockchain context. A choice for the custody agreement between investor and crypto-custodian should therefore determine the law that applies to security interests in digital assets under the control of the custodian.

However, the Hague Securities Convention restricts the choice to the law of states in which the custodian has an office that is either engaged in a business or regular activity or that is clearly identified in the securities account agreement. This restriction does not make much sense in the blockchain context, in which custodians do not have a network of offices around the world that are visited by customers, but exercise their business exclusively virtually. This is not to deny that there may be physical offices. The crypto exchange Coinbase, for instance, has a number of offices around the world. But it is unlikely that the administration of clients' accounts is done there. Rather, it is done virtually, *i.e.* on the blockchain. We believe restricting a choice of law by trying to attach it to a certain physical presence will unnecessarily complicate matters, give rise to legal arguments and thus increase legal uncertainty. As a matter of principle, the existence of an office should therefore not limit the possibility of choice of law and parties should be free to choose any law.

If no law has been chosen, the Hague Securities Convention refers to the office of the intermediary that has been specified in the account agreement.[23] Because crypto-custodians do not typically have widespread brick-and-mortar

21 The Hague Convention on the Law Applicable to Certain Rights in Respect of Securities Held with an Intermediary of 5 July 2006 ("Hague Securities Convention").

22 *Id.* at Art. 4(1).

23 *Id.* at Art. 5(1).

presence, such an office will only rarely exercise specific tasks on the blockchain. Even where they have offices, it is unlikely that these offices will perform any administrative tasks regarding the digital assets held for investors, because this is commonly done virtually, *i.e.* on the blockchain. Yet there are exceptions. For instance, the website blockchain.com separates customers according to their country of residence and the services provided, and assigns them to different country offices.[24] This may well indicate an implicit choice of law.

Failing a choice of law or a specified office, the Hague Securities Convention refers to the law under which the intermediary is incorporated or organised or has its principal place of business.[25] Even though a crypto-custodian may not have an office, it must have a state of incorporation, so that this connection factor may also work in the context of digital assets. In particular, a crypto-custodian such as a wallet provider or crypto-exchange will virtually always be incorporated under the law of some jurisdiction, and may also have a principal place of business. For instance, Coinbase Global Inc. is incorporated under the law of Delaware, notwithstanding the fact that the company hails itself as having become a "remote-first company."[26]

What if these connecting factors fail, *i.e.* if no choice has been made and the crypto-custodian's place of incorporation or principal business cannot be determined? In this case, it seems impossible to identify the governing law by reference to the custody agreement or the custodian, and other connecting factors must be sought. These will most likely be the same as those used for digital assets that are not controlled by a custodian, which is the topic of the next section.

4 Custody-Free Digital Assets

Where assets are not controlled by a custodian, one must use other connecting factors. This applies to digital assets directly held on the blockchain, and the private key of which is stored on a computer, on an external hard disk or flash

24 See "Blockchain.com User Agreement" <https://www.blockchain.com/legal/terms> accessed 8 April 2022.

25 See the Hague Securities Convention (n 21), Art. 5(2) (submitting intermediated securities to the law under which the intermediary is incorporated or otherwise organised, or, failing such incorporation or organisation, to the law of its principal place of business).

26 See Coinbase Global Inc., "Registration Statement under the Securities Act 1933 with the SEC" (*SEC*, 25 February 2021) <https://www.sec.gov/Archives/edgar/data/1679788/000162828021003168/coinbaseglobalincs-1.htm>.

drive. The same is true when the custody law cannot be identified, because no law has been chosen and the place of incorporation or principal place of business of the custodian cannot be determined.

4.1 *Choice of the Applicable Law?*

Secured transactions are often embodied in a formalised agreement. Such an agreement may contain a choice of the applicable law and the competent court. This is also true for the many "staking agreements," as discussed above. An example is the "Nomination Agreement" by Pure Stake, which provides under the title "Governing Law; Dispute Resolution" the following *inter alia*:

> This Agreement shall be interpreted, construed and enforced in accordance with the internal laws of the Commonwealth of Massachusetts, without regard to its conflict of laws principles.[27]

As already implied above (see *supra* section III), most PIL regimes will honour party autonomy here, *i.e.* the choice that parties have made to govern their secured transaction. More specifically, it seems virtually uncontested that party autonomy is to be allowed when it comes to contractual aspects, *i.e.* the *inter partes* aspects, of such secured transaction. These *inter partes* aspects include the interpretation of the contract, what constitutes default, *etc.*[28] Party autonomy is even allowed where the contract forms the basis for the creation of security rights. Thus, the fact that property law in most jurisdictions is largely mandatory law and applies notwithstanding any contractual arrangements, does not exclude the application of the principle of party autonomy to the contractual aspects of secured transactions, except in situations that are exclusively connected to one country.[29] The contractual rights and obligations

27 See PureStake, "Nomination Agreement" (*PureStake* 22 October 2019), No 21 <https://www.purestake.com/staking-agreement/>.

28 But see, *e.g.*, Katharina Pistor, *The Code of Capital: How the Law Creates Wealth and Inequality* (Princeton: Princeton University Press 2019) who is highly critical of party autonomy where it concerns PIL, especially in the context of corporate and property law.

29 See sec. 187(2) Restatement (Second) Conflict of Laws (allowing the parties, safe for some exceptions, to choose the law to govern their contractual rights and duties "even if the particular issue is one which the parties could not have resolved by an explicit provision in their agreement directed to that issue"), Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), [2008] OJ L 177/6, Art. 3(3) ("Rome I Regulation") (providing that a choice of the parties shall not prejudice the application of mandatory rules where all other elements relevant to the situation at the time of the choice are located in a country other than the country whose law has been chosen). See also United Nations, *United*

under a secured transaction, *i.e.* the *inter partes* aspects, are thus to be determined by the chosen law.[30]

A trickier question is whether party autonomy is also to be allowed when it comes to the proprietary aspects of the transaction, *i.e.* the *erga omnes* aspects. These *erga omnes* aspects include the creation and perfection of security rights, and the priority between proprietary rights. Serious objections seem to militate against this possibility. It could violate, first, the principle of *privity of contract*, according to which an agreement between two parties cannot have effects against third parties who were not taking part in the agreement.[31] Second, the choice made is not always easily identifiable for third parties, who would have to rely on the allegations of the parties to the contract.[32] Third, the possibility of choice could open up avenues for fraudulent manipulation. For instance, the parties to a secured transaction could choose a law that backdates the finality of the transferor in order to disenfranchise a transferee of an earlier transaction.

Against all these objections, equally valid counter arguments could be formulated: first, privity of contract is not absolute, and even in contract law, it is generally acknowledged that contracts may have legal consequences for third parties, who may thus either rely on those contracts or (unjustifiably) suffer from them. Second, in several instances, contractual agreements with third party effects are also not considered problematic in other situations, provided it is not impossible that they become identifiable, for instance by court order or attachment. An example would be the situation described above, *i.e.* when third parties try to acquire or seize specific digital assets, and have to learn

---

Nations Convention on the Assignment of Receivables in International Trade (New York: United Nations Publications 2001), Art. 30(2) (clarifying that mandatory of the law of the forum or another state may not prevent the application of the law of the state in which the assignor is located).

30 See UNCITRAL (n 15), Art. 84 (allowing a choice of law for "the mutual rights and obligations of the grantor and the secured creditor arising from their security agreement"). See also Swiss Federal Act on Private International Law (PILA) of 18 December 1987, SR 291, AS 1988 1776, Art. 105 (subjecting the pledging of claims, securities and other rights to the law chosen by the parties, with the explicit proviso that the choice cannot be asserted against third parties).

31 On privity of contract, see *e.g.*, Ewan McKendrick, *Contract Law* (10th edn, Oxford University Press 2022); Chris Turner, *Contract Law* (2nd edn, Hodder Education Group 2007), 48 et seq.

32 Eva-Maria Kieninger, "Freedom of Choice of Law in the Law of Property?" (2018) 7 European Property Law Journal 221 (arguing against choice of law in property law in general); Harry C. Sigman and Eva-Maria Kieninger, "The Law of Assignment of Receivables: In Flux, Still Uncertain, Still Non-Uniform," in Harry C. Sigman and Eva-Maria Kieninger (eds.), *Cross-border Security Over Receivables* (Sellier European Law Publishers 2009).

through attachment order with which custodian these assets are held. Third, possibilities of fraud are always present, and should not determine our preference of one rule over another. For instance, fraud is equally possible – and sometimes to much greater negative effects – where it regards the contractual aspects of transactions. Moreover, manipulations of the applicable law can, as always, be countered with the exception of fraud, which also applies in conflicts of laws (see in that sense the concept of *fraude à la loi*).[33]

Be this as it may, many PIL regimes are reluctant to allow party autonomy for proprietary aspects, although prominent exceptions exist.[34] However, the blockchain environment, because of its technical nature, may require a solution that derogates from the traditional views just summarised. For instance, the residence of the transferor at the time of the transfer may be even more difficult to identify than the law to which the parties have subjected their agreement. To exclude the uncertainty connected to the location of the transferor, the transferee in a secured transaction may want to choose the applicable law or fix the location by agreement. This seems legitimate from the perspectives of legal certainty and predictability, which, as already stated above, should be the leading principles in the context of proprietary rights. The same considerations informed the drafters of the Hague Intermediated Securities Convention, as it allows, with certain limits, to choose both the applicable law to proprietary rights and the location of the intermediary (see *supra* section 3). The interests of third parties can then be protected by requiring sufficient evidence about such a choice, *e.g.* that it must be made in writing or in electronic form. They may further be safeguarded by a universal requirement that the transferor must lose "control" over the digital assets as a result of the secured transaction (see in more detail *infra* section 5).

In sum, we argue that the choice of law of the parties should govern not only the contractual aspects of the secured transaction (*i.e.* the *inter partes* aspects), but also the proprietary aspects (*i.e.* the *erga omnes* aspects). According to many, the law that applies to a blockchain as a whole can also be chosen,

33 On this, see *e.g.*, Bernard Audit and Louis d'Avout, *Droit International Privé* (8th edn, L.G.D.J. 2018), 269 et seq.

34 See Kieninger (n 32). See also European Law Institute, "EU Principles on the Use of Digital Assets as Security" (*ELI*, February 2022), footnote 44 <https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_the_Use_of_Digital_Assets_as_Security.pdf> (arguing that "allowing the parties to a security agreement to choose the law applicable to third-party relations … would be inconsistent with some of the basic tenets of property ”aw"). See Uniform Commercial Code (UCC) Article 8 and the Hague Securities Convention (n 21), as well as the Dutch Civil Code Art. 10:135 (Debt-claim to name) which regards the property law aspects of assignment of claims.

for instance in terms and conditions downloaded with the blockchain software and accepted by the user (node).[35] How do these types of choices relate to each other? According to the principle of independence discussed above (see *supra* section 2), the law applicable to the chain and to the secured transaction must not necessarily be the same. Nevertheless, where a law governing the blockchain has been explicitly chosen, such choice will usually have been intended to cover all operations on this chain. It seems difficult to imagine, or at least highly impractical if such a choice would leave the parties the freedom to agree to another law for an individual transfer or creation of security interests. In other words, we would argue that by accepting the terms of the blockchain, the parties also accept the predominance of the choice of law clause in it, including where it regards the requirements for validity and effects of security rights in digital assets recorded on that same blockchain.

A choice of law of the blockchain as a whole will thus most of the time exclude a different choice for an individual secured transaction. However, this predominance of the choice of law for the blockchain over the choice of law for the secured transaction is not absolute. Should coders of the blockchain or drafters of its terms and conditions wish to leave the choice of the law applicable to secured transactions to the parties of such transactions, there is no reasonable ground to deny this possibility. In the end, determining whether a separate choice of law is possible for secured transactions is thus a matter of interpretation of the choice-of-law clause for the blockchain as a whole.

4.2 *Law Applicable in the Absence of a Choice*

When digital assets are not "held" in custody and the parties have not chosen the law applicable to a secured transaction, there is no significant connection of the transaction as such to the law of a country. Instead, the governing law can only be found via the location of the parties involved, unless international principles of substantive law can be relied on. Absent such principles, and for want of a better connecting factor, one must necessarily refer to the location of one of the parties, if the digital assets are held on a permissionless blockchain and no choice of law has been made for the blockchain as a whole or the secured transaction specifically. The same is true where the law applicable to custody cannot be determined (see *supra* section 3).

The relevant parties in a secured transaction are: (1) the security provider; and (2) the security taker. Should we have to choose between the location of

35 See Andrew Dickinson, "Cryptocurrencies and the Conflict of Laws," in David Fox and Sarah Green (eds), *Cryptocurrencies in Public and Private Law* (Oxford University Press 2019).

either one of those parties, the location of the security provider seems to be preferable. A first reason is that the security provider is necessarily only one person, whereas it is not to be excluded that different persons in different jurisdictions may allege to be security takers and that a single law is needed to decide between those competing claims (see *supra* section 2). When there is a dispute over who acquired the better (security) right, the security provider is thus a more appropriate criterion than the security taker. Moreover, in a blockchain context, the identity or location of the security taker is often not known. For example, assets that are staked to a DeFi platform: it may be very difficult if not impossible to identify the place of incorporation or business of such a platform, its operator or coder. In contrast, it will be much easier to identify the customer of such a platform. In fulfilling the Know-Your-Customer duties, the platform or the crypto service provider that acts as its agent would need to inquire not only about the identity but also about the place of residence of the customer/security provider.

Additional arguments for the security provider's location as a connecting factor can be found in several texts of uniform law. For instance, the UN Convention on the Assignment on Receivables refers to the location of the assignor to determine the law governing priority rights.[36] The same connecting factor can be found in the Proposal for an EU Regulation on the law applicable to third-party effects of assignment.[37] If the assignment is done in the context of a secured transaction, the assignor is in effect the security provider. The UNCITRAL Model Law on Secured Transactions refers more generally to the law of the state in which the grantor is located to determine the creation, effectiveness against third parties, and the priority of a security right in an intangible asset.[38]

Certainly, there are also undeniable problems with the application of the law of the security provider's location. First, the location of the security provider may be not be readily identifiable for third parties. But so is the location

36 United Nations (n 29), Art. 30(1). *Cf.* also the proposal of 12 March 2018 of the EU Commission: Proposal for a Regulation of the European Parliament and of the Council on the law applicable to the third-party effects of assignments of claims, COM/2018/096 final - 2018/044 (COD).

37 Proposal for a Regulation of the European Parliament and of the Council on the law applicable to the third-party effects of assignments of claims, [2018] COM/2018/096 final, Art. 4(1).

38 UNCITRAL (n 11). It is to be noted that, pursuant to Art. 90 of the Model Law, the "location" of the grantor refers in a subsequent and alternative order to the state of the place of business, the state where the central administration is exercised, or the state of habitual residence.

of the security taker, which is why we generally favour the application of the law chosen by the parties (see *supra* section IV(1)). Only where such an explicit choice is absent, the better arguments speak in favour of the security provider's location. It is also often criticised that the location of the security provider may change. While this is true, it is also true for the location of the security taker, which is yet an additional argument to allow the parties to determine the applicable law by choice.

In the end, it seems a necessary choice between two evils, and the security provider's location, while far from perfect, seems to be less bad than the security taker's location. This is also the choice that the European Law Institute has made in its recently adopted Principles on the Use of Digital Assets as Security.[39] A more attractive, third option, however, may be to rely on international principles of substantive law as *règles matérielles de droit international privé* (see on this solution also *infra* section 5).[40] This would avoid all arguments just discussed against either one of the parties' location, but unfortunately, no such international principles exist as of yet. This may change in future, when UNIDROIT will have adopted principles that are currently being drafted and negotiated in the context of their Digital Assets and Private Law Project.[41]

In sum, at present the law of the security provider's location should be used as the residual connecting factor to determine the law applicable to security rights in digital assets. However, it must be stressed that its importance is limited. It only applies provided that: (1) the digital assets are not recorded on a permissioned blockchain that is operated and/or supervised in one single state; (2) the digital assets are not held by a custodian; and (3) no express choice has been made for either the law governing the blockchain, or for the law governing the secured transaction. Only if all these conditions have been satisfied, one must necessarily refer to the location of the security provider, for want of a better criterion such as international principles of digital assets law. These latter principles may become available in the foreseeable future, and if they materialise, they should be preferred as a residual over the law of the security provider's location. The same is true where digital assets are held in custody and the custody law cannot be determined.

---

39 See European Law Institute (n 34), Principle 3.

40 Dominique Bureau and Horatia Muir Watt, *Droit international privé* (5th edn, Presses Universitaires de France 2021), 672–685, 540-1–551.

41 See UNIDROIT, "Digital Asset and Private Law project" (*UNIDROIT*) <https://www.unidroit.org/work-in-progress/digital-assets-and-private-law/> accessed 7 April 2022. (Full disclosure: both authors of the present chapter have been involved in this project).

5 Good Faith Acquisition and the Requirement of "Control"

Under most legal systems, a party that acquires an asset without knowing that it is encumbered with a security right will receive property unencumbered.[42] This is known as the principle of good faith acquisition. It must also apply with even more force to digital assets, because otherwise trading on blockchains would be subject to incalculable risks and would eventually stall. The law that governs good faith acquisition must be determined in the same way as that for any other acquisition. It will thus depend on the crypto-custodian, a choice of law, and the location of the transferor.

The specific problem here is that the content of the law governing the good faith acquisition is not necessarily known in advance. Although unlikely, it is possible that a law has little or no requirements for such acquisition. Consequently, it is theoretically possible that this law allows good faith acquisition of a digital asset encumbered with a security right without the transferor having given up any control over the asset. In this case, the creditor/security taker could assert its security right in the debtor's/security provider's insolvency, only to find that the relevant digital assets have been transferred to another party. Even worse, a creditor/security taker could claim to have obtained *bona fide* a security right that ranks higher than another security right in the same asset that the debtor has created before.

In the case of tangible assets, this problem is of minor importance because, according to the *lex rei sitae* principle, the law governing property rights, including security rights or rights *in rem*, is that of the state where the asset is located. The general public will usually know whether this law requires any condition for a secured transaction as to the publicity or transfer of control, and will take the necessary precautions. This is fundamentally different in a digital environment that has no location and where a multitude of different property laws may apply. In such environment, it is indispensable that a uniform indicator exists that signals to the general public the possible existence of a security right. Otherwise, the *erga omnes* effect of such rights could be hardly justified.

Such a signal can take various shapes and forms, depending on the technological specificities of the blockchain in question. One could imagine, for instance, some sort of colouring of coins and tokens that are encumbered, which would be visible to all users. The simplest way to indicate the existence of

42 See on good faith acquisition from a comparative law perspective: Michele Graziadei and Lionel Smith, *Comparative Property Law: Global Perspectives* (Edward Elgar Publishing 2017).

a security right, however, is to require a loss of control by the security provider. This rough method avoids a second disposition by the security provider that would contradict the prior creation of the security right. The security provider could not effectuate such a second disposition because he would lack the necessary control.

Crucially, taking the loss of control as the relevant criterion is in line with the functioning of the blockchain. The technology that underpins the blockchain, the DLT, gives power to the party that is in control of a digital asset. Such control can be exercised, for instance, via a private key. The party having control has factual spending power, whereas others have not. It can transfer assets to others. Such transfers can also be made in the context of a secured transaction.

The law must not contradict the technology underpinning the blockchain and replace it with an entirely different legal analysis. Such an approach would put the functioning of the blockchain into danger and largely deprive it of its usefulness.[43] As a matter of principle, we believe, the law should not stand in the way of technology and commerce, but facilitate it.

Absent special techniques such as colouring of digital assets, which must be uniformly applied and be visible to all users, the creation of any security right on the blockchain must be accompanied by a transfer of control over the digital asset. At a minimum, the security provider should lose control over the digital asset so that he is prevented from transferring the relevant digital assets to another party or encumbering it again. There may be different technical means to achieve such a limitation of control, *e.g.* lock-up, blocking, bonding or freezing.

The question remains how the requirement of a loss of control can be imposed where the law governing the secured transaction does not require it. A traditional method under many conflict-of-laws regimes is to assume that a national law which allows for a secured transaction without any such loss is contrary to public policy (*ordre public*). Yet the threshold for violation of public policy is generally high. Thus, it would be difficult to argue that such a law "outrages its [the forum's] sense of justice and decency"[44] or that it would "violate some fundamental principle of justice, some prevalent conceptions of

43 Matthias Lehmann, "Who Owns Bitcoin? Private Law Facing the Blockchain" (2020) 21 Minnesota Journal of Law, Science & Technology 93, 116–120. Primavera De Filippi and Aaron Wright, *Blockchain and the Law: the Rule of Code* (Harvard University Press 2018), 193–204.

44 *Re Fuld's Estate* (*No 3*), [1968] P 675, at 678.

good morals, some deep-rooted tradition of the common weal."[45] In addition, public policy is not the right method here, because for this principle to apply, the result of the application of a foreign law must violate public policy, and as a matter of principle, a foreign law is not to be discarded for its abstract content.[46]

A technique to impose such universal substantive requirements has been developed in France. It is called the substantive rule of PIL (*règle matérielle de droit international privé*).[47] Such substantive rules are increasingly necessary due to the globalisation of exchanges, which calls for the surmounting of national idiosyncrasies and the application of uniform standards in various sectors.[48] This is particularly true for societal sub-systems that are completely devoid of any significant connection to a particular state. The blockchain is a prime example of such a societal sub-system. Its very nature as an a-national transfer mechanism calls for the establishment of a minimum of global rules.

As already indicated above, such global rules are currently elaborated by the UNIDROIT Working Group on Digital Assets.[49] The definition of control it uses could provide the basis for a world-wide substantive condition for the validity of secured transactions in particular. Such a requirement would greatly help the transparency of security rights to third parties. It would be an indispensable tool to justify the effect of such security rights against the whole world (*erga omnes*).

In sum, the validity of *any* secured transaction should be conditioned on a loss of control by the security provider. This condition is required independently of the content of the law that governs the transaction. The latter will thus merely determine other issues, in particular the existence of an agreement between the parties and the consequences of any defects of such agreement, *e.g.* in case of mistake, fraud or duress.

6 The Laws Applicable to Other Issues

We have so far identified two sources that govern a secured transaction and the validity and effects of security rights in digital assets: the national law applicable to the transaction as such, as well as a substantive rule of global

45 *Loucks v Standard Oil of New York*, 224 N.Y. 99, at 111 (1918), per Justice Cardozo.

46 Bureau and Watt (n 40), 457–458; Dicey, Morris and Collins, *Conflict of Laws* (15th edn, Sweet & Maxwell, 2018), 5-005–5-007.

47 Bureau and Watt (n 40).

48 See Gunther Teubner, "Global private regimes: neo-spontaneous law and dual constitution of autonomous sectors in world society?," in Karl-Heinz Ladeur (ed.), *Public Governance in the Age of Globalization* (Routledge 2017), 71–87.

49 UNIDROIT Digital Asset and Private Law project (n. 41).

PIL regarding control. Besides these two sources, there are other laws that may have an effect on the validity of the transaction and thus, on the validity of the security rights created by that transaction.

One example of such laws relates to those governing the capacity of the parties. The security provider or the security taker can be under incapacity to enter into contracts under the national law applicable to them, for instance because one has not attained the legal age required or is suffering from mental disturbance. These issues are usually submitted to the "personal law" of the party in question, which is ordinarily the law of its nationality or domicile.[50] This law may deviate from that governing the secured transaction.

Another example is insolvency law. The rules on avoidance may affect the validity of transactions, especially those that are concluded in the "suspect period" or "twilight zone" in which the debtor is insolvent but insolvency proceedings are yet to be opened. These transactions may be void or voidable. The rules on avoidance are those of the country in which the insolvency proceedings have been opened, or *lex fori concursus*. This may be the country in which the debtor has its establishment, its principal place of business or its centre of main interest (COMI), but it is also sufficient that he has at least some assets there.[51] In each of these cases, this law may differ from the law governing the secured transaction, as well as from the law governing the capacity of the parties.

Although they considerably complicate the picture, these additional rules have to be respected as well. Otherwise, the interests of minors, adults in need or the other creditors would be disregarded. Even in a digital environment, these parties deserve protection. That the validity of a secured transaction will as a result be subject to a number of different laws is a price that must be paid.

7 Conclusion

The results of this study can be summarised in the following list. A secured transaction, and the validity and effects of security rights in digital assets must be governed:

1. if the transaction is done on a blockchain or a protocol that is governed exclusively by one law, for instance the law of the central operator or the law of an authority that supervises the network, by that law;

50 Paul Torremans et al. (eds), *Cheshire, North and Fawcett: Private International Law* (15th edn, Oxford University Press 2017), 145 et seq; Bureau and Watt (n 36), 629 et seq.

51 See UNCITRAL (in cooperation with UNIDROIT and HCCH), *Legislative Guide on Insolvency Law* (New York: United Nations Publications 2005), 41–43.

2. where 1 does not apply and the transaction concerns a digital asset that is held by a custodian
    a. by the law chosen in the custody agreement; or
    b. where (a) does not apply, by the law of the state in which the custodian is incorporated or has its principal place of business;
3. where 1 and 2 do not apply, by the law the parties to the secured transaction have chosen, subject to the globally uniform requirement that the security provider must have lost control over the digital asset (see *infra*);
4. where 1, 2 and 3 do not apply, by the law of the security provider, again subject to the globally uniform loss of control requirement (see *infra*), and provided no internationally accepted principles of digital assets law are available. Should the latter become available, those principles should govern.

In the latter two cases, the secured transaction and the creation of security rights are effective under the condition that the security provider has transferred or at least lost control over the relevant digital assets. This requirement does not apply in the two cases on the top of the list. In these cases, the law governing the secured transaction is sufficiently identifiable by third parties so that they can investigate its content. This does not mean that a loss-of-control requirement would not be useful also in these circumstances. Its precise form and shape or the choice of a potential alternative must however be left to the national legislator whose law applies.

CHAPTER 17

Do Smart Contracts Need New Conflict-of-Laws Rules?

Mehdi El Harrak

1 Introduction

The law applicable to smart contracts is a new and fascinating problem for Private International Law (PIL) experts. Smart contracts, or self-executing computer code, are one of the major applications of distributed ledgers. Their legal characterisation is not obvious particularly as they have different uses within distributed ledgers. In addition, a distributed ledger and its related transactions may not have a connection with a precise legal system.

The question this chapter seeks to answer is whether traditional conflict-of-laws rules are suitable to handle smart contracts. One of the purposes is to make suggestions on which conflicts-of-laws rules should be used for smart contracts, or, if none is fitting, which new rules should be introduced. By adopting a PIL approach, these questions will be analysed in three steps: the characterisation of smart contracts (section 2), the potential connecting-factors (sections 3 and 4), and overriding mandatory rules (section 5).

2 Characterisation of Smart Contracts in PIL

2.1 *General Description*

Nick Szabo, an American computer scientist, defined smart contracts as "computerized transaction protocols that execute terms of a contract."[1] He further explained: "the general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimise exceptions both malicious and accidental, and minimise the need for trusted intermediaries. Related economic goals

1 Nick Szabo, "Smart Contracts" (*FON*, 1994) <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html> accessed 8 July 2021.

© MEHDI EL HARRAK, 2023 | DOI:10.1163/9789004514850_019
This is an open access chapter distributed under the terms of the CC BY-NC-ND 4.0 license.

include lowering fraud loss, arbitration and enforcement costs, and other transaction cost."[2]

In other words, smart contracts are computer protocols that will selfexecute when one or more predefined conditions are met. They are typically used to automate the execution of a transaction so that all participants can be immediately certain of the outcome, without any intermediary's involvement or time loss. Their operating principle is simple: if certain conditions are met, the computer protocol will self-execute, without any intervention. Indeed, they are often presented as following the "if …then" principle. "Smart contracts roughly follow the scheme 'if x, then y', which in a basic design recalls a sort of digital vending machine."[3] It is easy to imagine that smart contracts could be very useful for the performance of an international transaction. In order to provide a brief overview of the potential uses of smart contracts, I will describe two possible situations.

As a first example, let's imagine contracting parties who choose to use a smart contract and a classical contract to settle various transactions. The smart contract is used because of the advantages it offers – certainty in performance of contractual obligations and no need for intermediaries. In short, the smart contract will help the execution of the legal contract, for instance, by automating a crypto payment in case of a specific event.

Now, let's suppose, in the example, that the smart contract automatically performed an erroneous transfer of cryptocurrencies in breach of the provisions of the legal contracts. In this situation, classical justice appears to be the only solution to reverse the effects of the smart contract. The intended effect – the execution of the contract – could be challenged on many legal grounds, for example on the basis of the theory of unjust enrichment. If, after the effects of the smart contract have been fully materialised, a party wishes to challenge this execution, it could turn to a state judge or an arbitral tribunal. This is not excluded by the technological irreversibility or "immutability" of the blockchain. "Though it is impossible to delete a block once it has been added to the chain, the law can reverse the effects of such transfer. The means for doing this is ordering a reverse transfer."[4] Such a reverse transfer could be ordered by a national judge or an arbitral tribunal as it would be for real-world contracts.

2 *Id.*

3 Pierluigi Cuccuru, "Beyond bitcoin: an early overview on smart contracts" (2017) 25 International Journal of Law and Information Technology 179, 185.

4 Matthias Lehmann, "Who Owns Bitcoin? Private Law Facing the Blockchain (EBI Working Paper Series No. 42)" (*SSRN*, 14 March 2020), 21 <https://ssrn.com/abstract=3402678>.

As a second example, let's imagine several environmental activists who want to raise funds to clean the ocean seabed using robots and artificial intelligence. Such a project could benefit from the use of a decentralised autonomous organisation (DAO).[5] The original DAO was described as "an organization that was designed to be automated and decentralised. It acted as a form of venture capital fund, based on open-source code and without a typical management structure or board of directors."[6] Technically, DAOs are based on smart contracts, which underlie their functioning: there are no contracting parties involved here nor binding intentions.

These two examples describe two radically different uses of smart contracts. In the first example, the smart contract helps the execution of a legal contract and may be, in consequence, subjected to a dispute. In the second example, the smart contract is used for technical purpose only as the "backbone of a DAO."[7]

2.2 *Different Types of Smart Contracts*

Before smart contracts can be characterised, it is necessary to have a look at the different types of smart contracts. The European Law Institute (ELI) proposes a set of Principles on the legal governance of blockchain and smart contracts.[8] According to their Principle 2, there are four types of smart contracts.[9]

2.2.1 Smart Contracts Used as Legal Contracts

The smart contract can be used as legal contract. As explained by the ELI, this raises the question of whether smart contracts can be regarded as legally binding if they are written as computer codes. Computer scientists understand self-executing computer code, whereas lawyers immediately focus on the word "contract."

In our opinion and following a functional method for the characterisation of smart contracts, when they are used as a legal contract by (human) contracting parties, they should be regarded as legal contracts and be therefore legally-binding if there is an offer and a corresponding acceptance in the legal

5 On the DAO, see Chapter 20 of this book by Florence Guillaume and Sven Riva, "Blockchain Dispute Resolution for Decentralized Autonomous Organizations: The Rise of Decentralized Autonomous Justice".

6 Nathan Reieff, "Decentralized Autonomous Organization (DAO)" (*Investopedia*, 24 September 2021) <https://www.investopedia.com/tech/what-dao/>.

7 Expression used by the distributed ledger Ethereum. See, for instance, their webpage: Ethereum, "Decentralized autonomous organizations (DAOs)" (*Ethereum*) <https://ethereum.org/en/dao/#how-daos-work> accessed 6 May 2022.

8 Sjef van Erp, Martin Hanzel, and Juliette Sénéchal, "Blockchain Technology and Smart Contracts" (*European Law Institute*), forthcoming <https://www.europeanlawinstitute.eu/projects-publications/current-projects/current-projects/blockchains/> accessed 22 June 2022.

9 *Id.* at 13.

sense.[10] Contracting parties should be free to prefer a smart contract as their *negotium* rather than a classical contract. As only the correspondence between offer and acceptance is required, traditional contract law will then apply either for a smart contract used as a legal contract or for a classical contract.

2.2.2 Smart Contracts Used as Mere Code without an Underlying Legal Agreement

Other smart contracts "merely perform status changes on the blockchain that lead to *de facto* changes without any further legal effect (*e.g.*, in the context of voting on proposals in the context of DAOs). Such smart contracts are not contracts in the civil law sense, but merely technical phenomena."[11] They are mere code, nothing more. These smart contracts are used as a technical tool by computer scientists within distributed ledgers. They can also be supported by artificial intelligence. There are no contracting parties involved. This type of smart contract is mere code without the participation of any human beings. They serve purely technical purposes. They will not be considered in this paper.

2.2.3 Smart Contracts Used as Tools to Execute Legal Contracts[12]

The third type of smart contract serves as a technical tool to perform a classical – *i.e.*, off-chain – legal contract. It could, for instance, execute the transfer of a certain amount of cryptocurrency where certain parameters are fulfilled. It is not binding under civil law,[13] and therefore should be regarded as totally different from smart contracts that are legal agreements. The latter are binding under civil law.[14]

2.2.4 Smart Contracts Merged with a Legal Agreement[15]

This fourth type of smart contract exists in two versions, "simultaneously both on-chain and off-chain."[16] It is perfectly illustrated by the so-called Ricardian contract, whose name is chosen as a tribute to David Ricardo, British political economist, and a major contributor to the theory of international trade during the 19th century. A Ricardian contract is a contract which exists in two identical versions, a normal version, *i.e.*, a classical contract, and an informatic version, *i.e.*, a smart contract. Contrary to smart contracts used as a tool to

10 *Id.* at 25.
11 *Id.* at 24.
12 *Id.*
13 *Id.* at 25.
14 *Id.* at 25.
15 *Id.* at 27.
16 *Id.*

execute off-chain legal contracts, the smart contract involved in a Ricardian contract makes the *off-chain* legal agreement completely executable *on-chain*. The Ricardian contract was originally proposed to record a financial instrument as a legal contract. Its purpose is to create a legal relationship which is readable by computer programs, and understandable by humans.

In sum, in the case of a Ricardian contract, two versions of a legal contract exist, one, written as computer code, *i.e.*, within a blockchain or "on-chain," and another outside of the blockchain, *i.e.*, a classical contract or "off-chain."

As a first step, the law applicable to the version of the Ricardian contract that exists in the legal world ("off-chain") must be determined. This seems rather easy insofar as the classic PIL rules for contracts may be used. In case of the absence of choice, conflict-of-laws rules will determine the applicable law to the real-world contract.

As a second step, the law so defined will be extended to the smart contract ("on-chain"). This step is based on the presumption that the smart contract is just the classic contract written in another language. Consequently, the law applicable to the legal agreement and the smart contract is the same. Theoretically, one may imagine a situation in which the content of the legal contract and the smart contract diverge. In such a situation, the legal contract should, in my opinion, prevail. This is in line with Principle 9 proposed by the ELI, titled "Off-chain prevails over on-chain." The explanation states that "where a contract, or elements of a contract, concluded outside the blockchain is translated into code [...], the terms of the contract concluded outside the blockchain prevail over any conditions coded on the blockchain, unless the parties have explicitly agreed otherwise outside the blockchain."[17]

The applicable law to smart contracts reflecting a legal agreement will then be the law normally applicable to the classic contract. In that sense, Ricardian contracts can therefore be neglected in the rest of this paper.

2.3 *Two Categories of Smart Contracts in PIL*

The remainder of this paper will focus on the two main types of smart contracts: those that are legal contracts and those that serve to execute a legal contract.

2.3.1 Smart Contracts Used as Legal Contracts

It is reasonably clear that smart contracts can be regarded as legal contracts where the "prerequisites for the conclusion of a contract in the respective legal system (*e.g.* offer and acceptance) are fulfilled."[18] This is the view of many

17 Van Erp, Hanzel, and Sénéchal (n 8), 35.
18 *Id.* at 26.

experts, including the UK Jurisdiction Taskforce (UKJT), according to which "there is a contract in English law when two or more parties have reached an agreement, intend to create a legal relationship by doing so, and have each given something of benefit. A smart contract can satisfy those requirements just as well as a more traditional or natural language contract. A smart contract is therefore capable of having contractual force. Whether the requirements are in fact met in any given case will depend on the parties' words and conduct, just as it does with any other contract."[19]

The first step to determine the law applicable to these smart contracts is to characterise them, as it is necessary for conflict-of-laws rules in general. For instance, if the object of the smart contract is the provision of a service, it can be characterised as a service contract, and the specific conflict-of-laws rules for service contracts can be applied.

2.3.2 Smart Contracts Used as Tools to Execute Legal Contracts

The second type of smart contract poses a more intricate problem. It is just a tool in the performance of a contract that exists outside of the blockchain. Given that there is no real "meeting of the minds" for this kind of smart contract, *i.e.*, no congruence between an offer and an acceptance, it cannot be regarded as a legal agreement.[20] The meeting of the minds takes place in a legal contract outside the blockchain. Consequently, these smart contracts should be characterised not as contracts, but as "acts of performance or settlement tools" for contracts.[21]

The functional method will allow us to precisely distinguish the category of smart contract involved. Two elements can be outlined: (1) the presence of contracting (human) parties, and (2) the kind of use of the smart contract (as a legal contract or as a technical tool to execute a legal contract).

The first element – the presence of contracting (human) parties – excludes the second type of smart contracts outlined by ELI – a technical tool for the maintenance of some DLT-features, such as a DAO – out. The second element – the use of the smart contract – will allow us to distinguish between smart contracts used as legal agreements and smart contracts used as tools to execute legal agreements.

---

19 UK Jurisdiction Task Force (UKJT), "Legal statement on cryptoassets and smart contracts" (*The LawTech Delivery Panel*, November 2019) <https://resources.lawtechuk.io/files/4.%20Cryptoasset%20and%20Smart%20Contract%20Statement.pdf> accessed 22 June 2022, at 8.

20 Van Erp, Hanzel, and Sénéchal (n 8), 24, 25.

21 *Id.* at 25.

In sum, smart contracts will be characterised differently for the purpose of PIL. They can either be contracts in the legal sense or acts of performance. The law applicable to them will differ accordingly.

3 Connecting Factors for Smart Contracts Used as Legal Agreements

3.1 *Preliminary Words*

Once a smart contract has been characterised as a smart contract used as a legal agreement, should it be subject to a law other than the one regulating real-world contracts performing the same transaction? In our view, it should not.

First, as previously seen, smart contracts are usually preferred over classical contracts as a result of several advantages – mainly, certainty in the performance and the absence of intermediaries. There is no reason these advantages should result in the application of a law other than the one applicable to the legal contract performing the same transaction.

Second, smart contracts are used for specific operations, such as international payments, insurance, financial trading, *etc*. These transactions are regulated at the national level. In other words, most of the transactions performed by smart contracts are already subject to substantive national laws.

Third, with a view to harmonising the conflict-of-laws rules, the transaction performed should be subject to the same applicable law, regardless of whether the agreement is a smart contract – when used as legal contract only – or a legal contract. Thus, according to Principle 4 a) on the legal governance of blockchain and smart contracts "transactions made on or supported by blockchain technology are subject to the rules of the law that would apply to functionally equivalent acts outside the blockchain; this includes all rules of private international law."[22] Without a doubt, this functional equivalence must be the primary focus when characterising smart contracts.

As a consequence, smart contracts used as legal contracts should be subject to the law that would be applicable to functionally equivalent legal contracts outside the distributed ledger. As previously seen, the problem encountered by geographically-dependant connecting factors in a DLT context, remains limited for smart contracts used as legal contracts. This use makes them closer to the parties, to their legal systems and to the transaction performed, than to distributed ledgers.

22 *Id*. at 28.

Their characterisation, based on the functional method, will lead to determination under the law that would normally be applicable to legal contracts performing the same transaction with the same foreign elements. Nevertheless, the next step, for the resolution of conflict of laws, is now to use the appropriate connecting factor.

As its name suggests, a connecting factor connects "a factual situation with the law of a specific jurisdiction."[23] In addition to providing a relevant connection, a connecting factor must be practicable in a DLT context. The classic connecting factors – such as the habitual residence of the party that delivers the characteristic performance – are quite flexible and adaptable. They may nevertheless encounter obstacles within the DLT ecosystem.

Against this backdrop, connecting factors adapted to the DLT system have been proposed by the Financial Market Law Committee[24] for one main reason: the difficulty localising digital assets in distributed ledgers. "Instead of focusing on the location of the asset or the place where the transaction was made, the focus is shifted to the location of the participant [...]."[25] However, the FMLC connecting factors deal with the *proprietary law* applying to crypto assets. Therefore, they are not relevant for smart contracts and will not be considered in this paper.

3.2 *Party Autonomy*

As these smart contracts are regarded as legal contracts, and "an eligible way to express the will of a party,"[26] the principle of autonomy should apply. However, there is a need for alternative connecting factors to the party's autonomy in the absence of choice. In this case, another connecting factor must be used to determine the applicable law. But which one?

3.3 *The Law of the Closest Connection*

In the absence of choice, the principle of the closest connection is applied in PIL to determine the applicable law. This "closest connection is generally best

23 Tim W. Dornis, "Connecting Factor," in Jürgen Basedow et al. (eds), *Encyclopaedia of Private International Law Vol 1 Entries A-H* (Cheltenham: Edward Elgar Publishing 2017).

24 A list of connecting factors adapted to the DLT ecosystem has first been introduced in an article written by the Financial Markets Law Committee (FMLC) published in March 2018. FMLC, "Distributed Ledger Technology and Governing Law: Issues of Legal Uncertainty" (*FMLC*, March 2018) <http://fmlc.org/wp-content/uploads/2018/05/dlt_paper.pdf> accessed 22 June 2022.

25 HCCL (2020), p. 4.

26 Van Erp, Hanzel, and Sénéchal (n 8), 26.

determined by the conflicts concept of characteristic performance,"[27] *i.e.*, the non-monetary obligation, a notion especially used by the European legislators.

In this context, it is helpful to have a look at the Rome I Regulation on the law applicable to contractual obligations. Its Article 4 on the "applicable law in the absence of choice" lists different types of contracts – *i.e.*, sale of goods (lit. a), service contracts (lit. b), contracts relating to immovables in general (lit. c), special tenancies (lit. d), franchise contracts (lit. e), distributorship contracts (lit. f), auction sales (lit. g) contracts concerning multilateral systems (lit. h) – and provides different connecting factors for them. For the majority of the listed contract types (lit. a, b, d, e, f), the determination of the applicable law is based on the general principle that the closest connection to a contract is determined by the characteristic performance.[28] Thus, according to Article 4 Rome I, contracts for the sale of goods, for the provisions of services, a tenancy of immovable, franchise contract and distribution contract[29] shall be governed by the law of the country where the party required to perform the characteristic performance has its habitual residence.

Could this connecting factor – the closest connection based on the concept of characteristic performance – be used to determine the law applicable to smart contracts? As previously mentioned, and in accordance with Principle 2 proposed by ELI, there should be no doubt that the existence of an offer and an acceptance are sufficient to characterise smart contracts as legal contracts. The characteristic performance under these smart contracts will be the non-monetary obligation, as is also usual for other contracts.[30] This method of determining the connecting factor will allow for a precise characterisation and subsequent application of the corresponding conflict-of-laws rule. As outlined, by ELI, "given the "if X, then Y-condition" of the smart contract, it must already be clear when the smart contract is deployed which performance is owed if the smart contract is triggered, e.g., by payment of a cryptocurrency amount. As a result, the smart contract will generally be determined in terms of its content"[31] and the characteristic performance will be identified accordingly.

---

27 Ulrich Magnus, "Article 4 Rome I Regulation: The Applicable Law in the Absence of Choice," in Franco Ferrari and Stefan Leible (eds), *Rome I Regulation* (Otto Schmidt 2009), 28.

28 *Id*. at 33.

29 The connecting factor for contracts relating to immovables in general is not the place of the characteristic performance, but the place of the immovable. This connecting factor will be dealt with separately.

30 The characteristic performance could be difficult to determine for some smart contracts, as it is already for legal contracts. These difficulties should be solved as they are solved for legal contracts for this type of smart contracts – smart contracts used as a legal contract.

31 Van Erp, Hanzel, and Sénéchal (n 8), 26.

It can be concluded at this point that the major difficulty is the characterisation of the contract and not the application of the connecting factors. These connecting factors refer for example to the location of a party, and not to that of a digital asset inside the network, which would be impossible to identify. Despite the potential problem of anonymity and/or pseudonymity,[32] geographically-dependent connecting factors remain relevant in a Distributed Ledger Technologies (DLT) context.

As an example, let us suppose smart contracts are used as legal contracts to regulate the sale of intangible goods. Within distributed ledgers, these intangible goods are digital assets. These digital assets could be exogenous tokens, *i.e.*, "tokens which have a necessary connection with assets existing outside the blockchain"[33] or endogenous tokens, *i.e.*, tokens which "do not refer to anything existing outside the blockchain."[34] These smart contracts are used as legal sales contracts. Once the smart contract used as a legal contract has been characterised – a sales contract – then the classical connecting factor will normally determine the applicable law – traditionally the law of the place of the habitual residence of the seller.

3.4 *The Lex Loci Contractus*

The *lex loci contractus* is the law of the place where the contract was made. In the absence of choice of law, it could provide a relevant connecting factor for smart contracts if the characteristic performance cannot be identified or if it is not used by the forum involved.

3.5 *The Lex Rei Sitae/Lex Situs*

The *lex situs* is relevant for tangible property, in particular for immovable property, but also for movable property. For instance, a smart contract could involve an automatic ownership transfer of tangible goods, immovables, or movables. In the absence of choice of law governing such a smart contract, the *lex rei sitae* is then relevant to determine the applicable law as it is for classical contracts.

To conclude on smart contracts used as legal contracts, they should be submitted to all rules of PIL that would normally apply to equivalent legal contract outside the blockchain by using the functional method for their characterisation.

---

32 On this particular subject, see Chapter 6 of this book by Anne-Grace Kleczewski, "The Good, the Bad and the Ugly - Private International Law, Crypto-Transactions and Pseudonyms".

33 The distinction between exogenous tokens has been drawn by Professor Gullifer. See UNCITRAL and UNIDROIT, "Joint UNCITRAL/UNIDROIT Workshop" (*UNIDROIT*, 6–7 May 2019), 2 <https://www.unidroit.org/english/news/2019/190506-unidroit-uncitral-workshop/conclusions-e.pdf>.

34 *Id.*

4 Connecting Factors for Smart Contracts Used as Tools to Execute Legal Agreements

As previously mentioned, smart contracts used as a tool to execute a legal agreement should be strictly distinguished from smart contracts used as legal contracts. Smart contracts, when used by identified (human) parties, can be broken down into the two categories. The first step for applying the corresponding conflict-of-laws rule is therefore a matter of characterising which type of smart contract is involved, as is usual in PIL.

If the smart contract is just a tool, *i.e.*, a technical instrument, then it will normally be subject to the law governing the contract which it helps to execute, as it should be for acts of performances.

However, this type of smart contract, as mere performance, could also be more connected to another legal system as it could have effect under a law other than the one chosen by the parties for the legal agreement. This disconnect from the legal agreement is a classic issue for international contracts: a contract, or a part of a contract, may be more closely connected to a different legal system than the one chosen by the parties or the one where it is performed. In other words, the scope of the law applicable to a legal contract should not automatically include the smart contract used in the act of performance.

The European legislator proposed a solution in the Rome I Regulation on the law applicable to Contractual Obligations in Europe at Article 12 on the scope of the law applicable to a contract. The first paragraph mentions the interpretation (lit. a), the performance (lit. b), the consequences of a total or partial breach of obligations (lit. c), the various ways of extinguishing obligations, and prescription and limitation of actions (lit. d) and the consequences of nullity of the contract (lit. e). The law chosen by the parties or determined by a conflict-of-laws rule apply to these matters in European PIL. In contrast, according to Article 12(2) Rome I, "in relation to the manner of performance and the steps to be taken in the event of defective performance, regard shall be had to the law of the country in which performance takes place." This rule may lead to an applicable law other than that applicable to the legal contract. This conflict-of-laws rule – the law of the country in which performance takes place – is generally called the *lex loci solutionis.* But where is the place of performance in a DLT context?

This leads us to the question of the place of performance of a smart contract used as a tool in a DLT context. Since it is immersed in the digital world, the place of performance is not *a priori* obvious.

An answer to this question might be found in the recent regulation on blockchain of the Principality of Monaco. In particular, pursuant to Article 5 of

the draft bill n°237,[35] the "Monegasque law is applicable to blockchains, smart contracts, algorithmic processes and cryptocurrencies which produce effects on the territory of the Principality of Monaco. The effect is deemed to occur in the territory of the Principality of Monaco if one of its constitutive facts or one of its consequences has taken place in this territory."[36]

This proposal makes a given territory a place of performance of a smart contract – without any distinction regarding the type of smart contracts – if one of its constitutive facts or one of its consequences has taken place in this territory. For instance, if a smart contract is used to perform the transfer of traditional or cryptocurrencies to a bank registered in a given country or for a delivery of goods to be performed in a given country, then this country will be the place of performance. Even if a general answer concerning the place of performance in a DLT context remains difficult to provide, the first step, as per the Monegasque legislation, could be the place of interaction with the real world. If there is such an interaction, the place of performance could be determined in the traditional way.

However, the question of the place of performance in a DLT context without an interaction with the real world remains.

Proposals have been made by several experts to determine the place of performance when this is totally immersed in a distributed ledger[37] and two conclusions have emerged.[38] First, the place of performance could be "the location where the cryptocurrency is after it has been transferred, if it is possible to identify such a place."[39] Second, it could also be, for instance, in the case of an on-chain cryptocurrency transfer, the location of either the "the transferor or the transferee."[40] This make sense for an on-chain digital asset transfer performed by the second type of smart contract – for instance if the transferee

35 Conseil National, "n°237 – Proposal for a law on blockchain" (*Conseil National*, 4 December 2017) <https://www.conseil-national.mc/2017/12/04/237-proposition-de-loi-relative-a-la-blockchain/> accessed 30 July 2021.

36 Translation from the French version: "Le droit monégasque est applicable aux blockchains (chaînes de blocs), aux smart contracts (contrats intelligents), aux entreprises processus algorithmiques et aux monnaies cryptographiques qui produisent des effets sur le territoire de la Principauté de Monaco. L'effet est réputé se produire sur le territoire de la Principauté de Monaco dès lors qu'un de ses faits constitutifs ou une de ses conséquences a eu lieu sur ce territoire."

37 See for instance, British Law Commission (Law Com No 401), "Smart legal contracts: Advice to Government" (*Law Commission*, 25 November 2021) <https://www.lawcom.gov.uk/project/smart-contracts/>.

38 *Id.* at 193.

39 *Id.*

40 *Id.* at 194.

resides in a country other than the one where the legal contract it helps to execute is performed. The total immersion of digital assets and their transfer(s) in a distributed ledger does not disqualify other connecting factors such as the location of the parties.

In my opinion, in this particular situation – a smart contract used as a tool to execute a legal agreement potentially more connected to another legal system than the one of the legal agreement it helps to execute –, the place of performance of a smart contract that governs the transfer of on-chain digital assets should be the country where the transferor or the transferee is located or domiciled, – even if these parties are not the ones to the legal agreements rather than the geographical localisation of the digital assets. Even if this localisation could be identifiable, this does not mean it will provide a relevant connection. For instance, the localisation of the nodes that "contain" the digital assets involved could not provide any relevant connection with a legal system. Indeed, these nodes are randomly localised all over the world. However, the location of the transferor or the transferee in another legal system than the one of the legal agreement demonstrates a better connection as it clearly establishes another connection with real-world actors – for instance the final beneficiary of the on-chain digital assets transfer.

In sum, the place of performance for smart contract used as a tool will be determined by the interaction with the real world for off-chain crypto assets and the place of real-world actors for on-chain crypto assets. The *lex loci solutionis* will then determine the applicable law.

5 Overriding Mandatory Rules

5.1 *Overriding Mandatory Rules for Smart Contracts Used as Legal Contracts*

Overriding mandatory rules are basically defined as "provisions the respect for which is regarded as crucial by a country for safeguarding its public interests, such as its political, social or economic organisation, to such an extent that they are applicable to any situation falling within their scope, irrespective of the law otherwise applicable to the contract [...]."[41]

In light of this, which overriding mandatory rules should apply to smart contracts used as legal contracts? The first answer, in line with what has been

41 Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), [2008] OJ L177/4, Article 9.1 ("Rome I Regulation").

said before: the overriding mandatory rules that would be applicable to functionally equivalent legal contracts outside the distributed ledger. Examples are smart contracts with weaker parties, such as consumer contracts or insurance contracts. Overriding mandatory rules protecting the weaker party should apply, as they would apply for a functionally equivalent legal contract.

The second answer will focus on financial contracts. These are of essential importance for DLT. In his famous paper, Szabo wrote about financial contracts: "these new securities are formed by combining securities (such as bonds) and derivatives (options and futures) in a wide variety of ways. Very complex term structures for payments can now be built into standardised contracts and traded with low transaction costs, due to computerised analysis of these complex term structures."[42] These could not only be legal contracts, but also smart contracts used to perform other contracts and Ricardian contracts.

This leads us to the following question: does the area of finance require overriding mandatory rules for such smart contracts? Examples of such overriding mandatory provisions in the area of finance are rules prohibiting money laundering, terrorism financing or tax evasion.[43] The necessity and consequences of overriding mandatory rules on a smart contract used as a legal financial contract are beyond the scope of this paper and should be the subject of a special study. However, in our view, overriding mandatory provisions in finance should, as a general matter, be recognised. In addition to rules prohibiting money laundering, terrorism financing or tax evasion, regulatory rules that serve the stability of the financial system should be considered as overriding mandatory rules by the judiciary or even by the legislator *ab initio* considering the huge potential of smart contracts in finance.

5.2 *Overriding Mandatory Rules for Smart Contracts Used as Tools to Execute Legal Agreements*

Should the overriding mandatory rules of the state apply where smart contracts used as tools to execute legal agreements have their effect? Of course, there is no issue if these overriding mandatory rules are based on the law of the forum. However, it could involve overriding mandatory rules of a foreign State if this type of smart contract has its effect under another law when applying the *lex solutionis*.

The Swiss legislators proposed a solution. According to Article 19(1) of the Swiss Private International Law Act, "if interests that are legitimate and clearly

42 Szabo (n 1).

43 Matthias Lehmann, "Private international law and finance: nothing special?" (2018) 3 Nederlands Internationaal Privaatrecht 3.

preponderant according to the Swiss conception of law so require, a mandatory provision of a law other than the one referred to by this Act may be taken into consideration, provided the situation dealt with has a close connection with that other law." In other words, the closest connection to another legal system justifies taking into consideration its overriding mandatory provisions.

In our opinion, the answer could not uniformly be either affirmative or negative. On a case-by-case basis, overriding mandatory rules of a foreign State could apply to smart contracts used as a tool to execute a legal agreement based on the particular effect, the specific legal field and the situation. Therefore, re-visiting the previous example of finance, overriding mandatory rules could be applied for issues like Anti Money Laundering, Combating the Financing of Terrorism or tax evasion. If a smart contract used as a tool to execute a legal agreement results in the transfers of cryptocurrencies to a bank, the overriding mandatory rules of its country of registration, for example those whose purpose is to detect and to combat money laundering activities, must apply.

6 Conclusion

Traditional conflict-of-laws rules can handle smart contracts. The legal characterisation must first be determined, followed by an assessment of the connecting factors, in order to handle this new feature of major importance. Furthermore, in our view, the difficulty encountered to regulate DLT transactions in general is rather a matter of lack of legal imagination than a matter of thinking that distributed ledgers should comply with classical national rules. Distributed ledgers should be accepted as they are, a reality, a powerful one, a necessary one, which allow new and various transactions without intermediaries. Questioning the validity of distributed ledgers or trying to set some legal conditions to their use will only result in failure. Users, and in particular computer scientists, would find other ways to secure their transactions. By contrast, the absence of intermediaries, including lawyers, is a guarantee of effectiveness. Lawyers should capitalise on this efficiency with a "business-first mind-set."

CHAPTER 18

Blockchain-based Negotiable Instruments: with Particular Reference to Bills of Lading and Investment Securities

Koji Takahashi

1 Meaning of "Blockchain-based Negotiable Instruments"

This paper will consider what the choice-of-law rules should be for issues pertaining to blockchain-based negotiable instruments.

The concept of "negotiable instruments" refers to instruments representing relative rights (namely, entitlements that may be asserted against a certain person) such as rights to claim the performance of obligations and corporate membership rights. Which instruments fall under this description depends on the applicable law. It covers, for example, "Wertpapier," defined by the Swiss Code of Obligations (Obligationenrecht) as any document with which a right is linked in such a way that it can neither be asserted nor transferred to others without the document (Article 965). The concept of "negotiable instruments" as used in this paper is broader than the same expression as ordinarily understood in English law. Under the latter, "negotiable instruments" ordinarily mean the instruments which allow a *bona fide* transferee to acquire a better title than what the transferor had. In this narrow sense, bills of lading are not negotiable instruments under English law[1] although they are under German and Japanese law.[2] As this paper will examine negotiable instruments in the wider sense,[3] it will cover bills of lading and investment securities within its scope of analysis.

1 The Law Commission, *Digital assets: electronic trade documents: A consultation paper* (*Consultation Paper 254*) (Crown 2021), para. 3.15.

2 § 932 of the German Civil Code (Bürgerliches Gesetzbuch (BGB); Articles 520–5, 520–15 and Article 520–20 of the Japanese Civil Code.

3 It is also acknowledged in England that there are broad and narrow senses of negotiability: Law Commission (n 1), para. 3.9.

© KOJI TAKAHASHI, 2023 | DOI:10.1163/9789004514850_020
This is an open access chapter distributed under the terms of the CC BY-NC-ND 4.0 license.

The concept of "blockchain-based negotiable instruments" refers to tokens issued on a blockchain which are meant to serve as negotiable instruments. This paper's main focus is on blockchain-based bills of lading and blockchain-based investment securities (called crypto-securities). This paper will not make any particular mention of promissory notes, bills of exchange or cheques since no notable trend for issuing them on blockchains is observed as of the time of writing (August 2021), but they are not excluded from its scope. Intrinsic or "native" tokens (namely, tokens of self-anchored value) such as cryptocurrencies are outside the scope of this paper[4] since they do not represent any relative rights.

2 Social Significance and Legal Hurdle

Negotiable instruments are useful to facilitate the assignment (either an outright transfer or an assignment by way of pledging) of the rights they represent. The assignment of such rights would, without negotiable instruments, have to follow cumbersome steps, including steps necessary for securing the *erga omnes* effect (the effect against the whole world). Negotiable instruments could, through their possession and transfer, simplify the steps for assignment.

Negotiable instruments in paper form are a clumsy tool as they are costly and time-consuming to handle and there is a risk of loss. The clumsiness could be reduced by digitization. There are, however, technological and legal hurdles.

The technological hurdle is how to guarantee the uniqueness of a negotiable instrument in an electronic environment. A negotiable instrument must be a unique object to ensure that only one person is entitled to assert the right represented by it. But the nature of an electronic record is such that it can be easily copied to create indistinguishable duplicates. Prior to the arrival of the blockchain technology or distributed ledger technology (DLT), the uniqueness of an electronic form of negotiable instrument could only be guaranteed by means of a central register. In this architecture, the trusted intermediary who maintains the register decides which records are true. Now, with the blockchain technology, it has become possible for the first time in history to reach a consensus on a single true version of electronic records on a decentralised platform. A token on a blockchain is subject to the exclusive control of the holder of the corresponding private key, with the result that no two persons could claim to hold the same token. In this architecture, the uniqueness of an

4 Except to the extent they shed a useful light on analysis. See section 5.6.3 *infra*.

electronic record can be guaranteed without the need to put trust in intermediaries. Like paper-based negotiable instruments, blockchain-based negotiable instruments may be traded on a peer-to-peer basis. Tokens serving the role of negotiable instruments will lay the foundation for a vital aspect of the token economy.

The remaining hurdle to the digitization of negotiable instruments is the absence of a good legal infrastructure. Unless the applicable law recognises blockchain-based tokens as negotiable instruments, they cannot be handled with confidence. Even if the parties to a transfer of such tokens have agreed to treat them as being equivalent to paper-based negotiable instruments, it would not be sufficient since third parties are not bound by their agreement. Whether the token economy will fly or not, therefore, depends much on the development of a good legal infrastructure. The latter concerns both substantive rules and choice-of-law rules. In what follows, this paper will first examine the emerging substantive rules for blockchain-based negotiable instruments. The remainder of this paper will then turn to the choice-of-law question.

3 Emerging Substantive Rules

3.1 *Bills of Lading*

Bills of lading are negotiable instruments, issued by the carrier of goods, which represent the right to claim the delivery of goods from the carrier. They are the backbone of seaborne trade in goods.

Since paper-based bills of lading are slow to be transmitted, they often do not arrive at the port of destination until after the goods have arrived. Consequently, the goods often have to be delivered without the presentation of bills of lading, which in turn can cause a myriad of problems. As such difficulties could be avoided with the use of electronic bills of lading, there were a number of attempts to digitise in the past decades. Prior to the invention of the blockchain technology, a central register was the only conceivable architecture for digitization. Due to its design as a closed system, a central-register bill of lading does not work seamlessly unless all the parties who have stakes become registered members. This membership requirement has been a major obstacle to the spread of electronic bills of lading. A breakthrough may, however, be in the offing with the advent of blockchain, which has made it possible to issue electronic bills of lading on a platform for the use of which no permission is required.[5]

5 See Koji Takahashi, "Electronic bill of lading on blockchain" (*Blockchain, Cryptocurrency, Crypto-asset and the Law*, 18 October 2015) <https://bit.ly/3t3Hudo>.

A paper-based bill of lading would be a mere piece of paper in the absence of recognition that it is legally a bill of lading.[6] Likewise, an electronic bill of lading would be a mere electronic record unless there is recognition that it is legally equivalent to a paper bill of lading. An agreement between the carrier and one of the cargo interests to treat an electronic record as equivalent to a paper bill of lading would not be sufficient since it is not binding on third parties.[7] The past projects of electronic bills of lading have been beset by the lack of legal recognition, which has resulted in the reluctance of banks to accept electronic bills of lading as adequate collateral. In most legal systems, the lack of legislative support continues to this day. Under Japanese law, for example, the provision on the creation of bills of lading (Article 758(1) of the Commercial Code) is silent on the possibility of using electronic records in contrast to the provision on seawaybills[8] (Article 770(3) of the same Code) which expressly acknowledges the possibility of providing an electronic record. Recently, however, some States have reformed their laws to give recognition to electronic bills of lading, including those based on blockchains. Some of such legal systems, as well as a few international instruments, will be examined below.

3.1.1 German Law

German law recognises a qualified electronic record as a bill of lading. When its Commercial Code (Handelsgesetzbuch) was reformed in 2013, provisions on electronic bills of lading were introduced in § 516. Paragraph 2 of that section provides that an electronic record which fulfils the same functions as a bill of lading is equivalent to a bill of lading, provided that it is ensured that the authenticity and integrity of the record are maintained. Paragraph 3 empowers the Ministry of Justice and Consumer Protection to issue an ordinance (Rechtsverordnung) to regulate the details of an electronic bill of lading. The Ministerial ordinance has not yet been issued but that should not stop the courts from recognising an electronic record as a bill of lading if it

6 This does not mean that a statutory definition of "bill of lading" is necessary for legal recognition. Under English law, to determine whether a document is a bill of lading, a court will consider certain characteristics of the document, including whether it is titled "bill of lading" and whether it contains information ordinarily found in a bill of lading. Law Commission (n 1), para. 3.32.

7 For a view to the same effect, see *id.*, para. 2.37.

8 Seawaybills, unlike bills of lading, are non-negotiable instruments since they do not represent the right to claim the delivery of goods but are mere evidence of the receipt of goods and the terms of a carriage contract.

meets the requirements as provided in paragraph 2.[9] As these requirements are expressed in technology agnostic language, blockchain-based tokens are not excluded from the qualified electronic records.[10] The electronic records recognised as bills of lading are subject to the provisions applicable to paper-based bills of lading (§§ 929 *et seq*. of the Civil Code (Bürgerliches Gesetzbuch)), including the provision permitting *bona fide* acquisition (§ 932).[11]

3.1.2 Swiss Law

Swiss law allows a bill of lading to be issued in the form of a blockchain-based token. Switzerland enacted in 2020 the Federal Act on the Adaptation of Federal Law to Developments in Distributed Ledger Technology (Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register) (hereinafter "DLT Act"). The Act made a number of changes to the Code of Obligations with effect from 1 February 2021.

Of particular relevance to bills of lading is Article 1153a. It was inserted by the DLT Act and provides that documents of title to goods such as bills of lading may be issued in the form of "ledger-based securities"[12] (*Registerwertrechte*, *droits-valeurs inscrits*) (paragraph 1). The "ledger-based securities" are defined by Article 973d, also inserted by the DLT Act, as a right which, in accordance with an agreement between the parties, is registered in a "securities ledger" (*Wertrechteregister*, *registre de droits-valeurs*) and may be exercised and transferred to others only via the securities ledger (paragraph 1). The technical requirements of a securities ledger are laid down (paragraph 2), including the requirements that its integrity is protected against unauthorised changes and that creditors must be able to view the ledger entries without the involvement of a third party. Although the Code of Obligation does not use the words "blockchain" or "distributed ledger," the official explanatory note for the DLT Act cites some examples of public and private blockchains which the Federal

9 David Saive, *Das elektronische Konnossement: Umsetzung der Anforderungen aus § 516 Abs. 2 HGB durch funktionsäquivalente Blockchain-Token* (Mohr Siebeck 2020), 64. For a contrary view, see Clyde & Co. LLP, *The legal status of electronic bills of lading: A report for the ICC Banking Commission* (ICC Banking 2018), 37 [Tim Schommer].

10 On one interpretation, the use of a private blockchain is required to fulfil these requirements: Saive (n 9), 190.

11 *Id.*, 79.

12 This is the expression used in the unofficial English translation of the Code published at the official publication site for Swiss federal law (https://www.fedlex.admin.ch/eli/cc/27/317_321_377/en; Federal Act on the Amendment of the Swiss Civil Code (Part Five: The Code of Obligations) of 30 March 1911, SR 220) ("Swiss Code of Obligations").

Council believes would satisfy the requirement of integrity.[13] There is, therefore, no doubt that blockchain-based negotiable instruments may qualify as "ledger-based securities."

The DLT Act also inserted in the Code of Obligations other provisions on various aspects of ledger-based securities, which would also be applicable to blockchain-based bills of lading. These include provisions permitting *bona fide* acquisition (Article 973e(3)) and provisions detailing the procedure for a cancellation declaration (Kraftloserklärung) (Article 973h). The latter would be useful where the private key for a blockchain-based bill of lading is lost.

The official explanatory note for the DLT Act states that Article 1153a is in line with the Rotterdam Rules (United Nations Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea), which Switzerland has signed but not yet ratified.[14] We will now turn to this Convention.

3.1.3 Rotterdam Rules

The Rotterdam Rules is an international convention adopted by the United Nations in 2008. Though not yet in force at the time of writing (August 2021), it embraces "negotiable electronic transport record" (Articles 8, 50 and 51(4)), a concept which covers electronic bills of lading. One of the underlying principles of the Rotterdam Rules is technological neutrality: the law should neither require nor assume the adoption of a particular technology. It follows that blockchain-based tokens are not excluded *a priori* from the concept of "negotiable electronic transport record." But only an electronic record that fulfils the prescribed requirements (laid down in Article 9) may qualify as such. These requirements are a manifestation of the principle of functional equivalence, a principle which treats only an electronic record fulfilling the essential functions of a paper document as legally equivalent to the latter. If these requirements are satisfied,[15] blockchain-based bills of lading are admissible under the Rotterdam Rules.

---

13 Botschaft zum Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register (27 November 2019), BBI 2020 233, (The Act entered into force 1 February 2021, RO 2021 33), 281.

14 *Id.*, 291.

15 For an analysis, see Koji Takahashi, "Blockchain Technology and Electronic Bills of Lading" (2016) 22 Journal of International Maritime Law 202, 207.

3.1.4 UNCITRAL Model Law on Electronic Transferable Records and the National Legislation Based on It

In 2017, the UNCITRAL (United Nations Commission on International Trade Law) adopted the Model Law on Electronic Transferable Records. It lays down the attributes which an electronic record needs to possess for it to be treated as legally equivalent to the corresponding "transferable document." Defined as a document that entitles the holder to claim the performance of the obligation indicated in it and to transfer the right to performance through its transfer (Article 2), a "transferable document" is broadly synonymous with a paper-based "negotiable instrument" in the sense used in this paper. Bills of lading are covered by this concept whereas investment securities, though logically covered, are excluded (Article 1(3)). The Model Law adheres to the principles of technology neutrality and functional equivalence. Accordingly, the attributes of an electronic record that it lays down reflects the function of a "transferable document." If these are satisfied,[16] a blockchain-based bill of lading is deemed to be legally equivalent to a paper-based bill of lading.

In describing some of these attributes, the Model Law requires the use of a reliable method to establish the exclusive control of an electronic record that replicates a transferable document (Articles 10(1)(b)(i)(ii) and 11(1)(a)). It lists a number of circumstances by reference to which the reliability of a method must be evaluated, including the existence of a declaration by an accreditation body (Article 12(a)(vi)), but it leaves the details of accreditation to national laws. To date, the Model Law has served as the basis for legislation in a few jurisdictions including Bahrain[17] and Singapore.[18] The legislation of these two jurisdictions gives some details as to the procedure, requisites, and effects of accreditation.[19]

---

16 For an analysis, see 高橋宏司「有価証券の電子化のためのブロックチェーン利用の法的課題―船荷証券と UNCITRAL モデル法に着目して―」 in (2020) 5 国際取引法学会年報 24, 29–36 (Koji Takahashi, "Legal Issues Arising from the Use of Blockchains for the Dematerialization of Negotiable Instruments: with a Particular Focus on Bills of Lading and the UNCITRAL Model Law" (2020) 5 Yearbook of the Japanese Association of International Business Law 24, 29–36).

17 The Law No. 55 of 2018 with Respect to Electronic Transferable Records (with effect from 1 February 2019) ("Bahraini legislation"). For an analysis, see Koji Takahashi, "Bahraini legislation based on the UNCITRAL MLETR" (*Blockchain, Cryptocurrency, Crypto-assets and the Law*, 21 March 2019) <https://bit.ly/3mUpy3w>.

18 Part IIA of the Singaporean Electronic Transaction Act (with effect from 19 March 2021) ("Singapore legislation").

19 Articles 15 to 17 of the Bahraini legislation (n 17); Articles 16O(2) and 16Q of the Singapore legislation (n 18).

3.1.5 English Law

At the time of writing (August 2021), English law does not give recognition to electronic bills of lading. The Law Commission has issued a consultation paper[20] which contains a draft bill to make provision for trade documents in electronic form to have the same effect as trade documents in paper form. The consultation paper makes a number of remarks on blockchains and DLT. If the proposed bill is enacted, qualified electronic bills of lading would have the same effect as paper bills of lading. It would entail that a person who becomes the lawful holder of an electronic bill of lading has transferred to and vested in him all rights of suit under the contract of carriage (§ 2(1) of the Carriage of Goods by Sea Act 1992). In contrast to German and Swiss law, examined in sections 3.1.1 and 3.1.2 above, a *bona fide* transferee of an electronic bill of lading would not acquire a better title than the transferor since paper bills of lading are generally subject to the *nemo dat* principle[21] under English law.[22]

3.2 *Investment Securities*

Investment securities include company shares and bonds. When issued on a blockchain, they are referred to by various names such as crypto-securities, tokenised securities, and security tokens. This paper will call them crypto-securities unless the context compels other appellations.[23]

Investors today typically hold dematerialised securities through a chain of custodians. They are exposed to custody risks and may, depending on the applicable law,[24] be prevented from exercising the rights which investors directly holding shares would be entitled to.[25] Since the blockchain technology

---

20 Law Commission (n 1), Appendix 4.

21 The principle of *nemo dat quod non habet* (no one can give what he has not got) means that a person who does not own property cannot confer it on another: Jonathan Law and Elizabeth A. Martin (eds), *Dictionary of Law* (6th edn, Oxford: OUP 2006), 354.

22 *Id.*, para. 3.15. See also the text accompanying (n 1).

23 For example, in discussing Swiss law, the phrase "ledger-based securities" will be used as it is an English expression adopted in the unofficial translation published at the official site (See (n 12)), though that phrase covers, not just crypto-securities (as will be noted in section 3.2.2 *infra*) but also other blockchain-based negotiable instruments such as bills of lading (as noted in section 3.1.2 *supra*).

24 *Cf.* In some legal systems, intermediaries standing between an investor and the issuer have no legal significance and the investor is treated as the direct owner of the securities: Roy Goode et al., *Explanatory Report of the Hague Securities Convention* (2nd edn, HCCH 2017), para. Int-22.

25 See, for example, the English case of *Eckerle v Wickeder* [2013] EWHC 68, in which the investors holding shares through a chain of intermediaries were denied entitlement to a remedy – either to have a shareholder resolution cancelled or to receive an order for the purchase of their shares - which would be available to investors directly holding shares.

allows for disintermediation, crypto-securities, like paper-based securities, may be held directly by the investors. A direct link between the issuer and the investors enables the issuer to identify the investors in real time and enables the investors to exercise their rights straightforwardly. In addition, if combined with smart contract functionality, a complex capital structure of a company can be administered automatically, without human intervention.[26]

Crypto-securities would be nothing but an electronic record unless they are recognised as legally equivalent to paper-based securities. An agreement between the issuer and an investor to treat them as equivalent to paper-based securities would not be sufficient since it is not binding on third parties. In some legal systems, crypto-securities may be recognised as legally equivalent to paper-based securities based on the interpretation of the existing law. In Austria, for example, the practice of issuing crypto-securities is premised on the understanding that they are securities under the existing law.[27] But legal uncertainty is likely to set in where there is no specific legislation. Thus in Japan, opinion is divided over the conditions under which a negotiable instrument may be created. A leading opinion considers that there must at least be customary law authorising the creation of a negotiable instrument.[28] This hurdle would be high for blockchain-based negotiable instruments since the practice of using blockchains for the purpose of emulating negotiable instruments is as yet far from established. Recently, a few States have introduced legislation that recognises crypto-securities. Three such legal systems will be examined below.

3.2.1 Liechtenstein Law

In Liechtenstein, the Token and TT Service Provider Act (Token- und VT-Dienstleister-Gesetz: TVTG) entered into effect on 1 January 2020. It introduced

---

There are also other disadvantages investors holding shares through intermediaries may suffer: see Eva Micheler, "Intermediated securities from the perspective of investors: problems, quick fixes and long-term solutions," in Louise Gullifer and Jennifer Payne (eds), *Intermediation and Beyond* (Oxford: Hart Publishing 2020), 1, 3.

26 Travis Laster & Marcel Rosner, "Distributed Stock Ledgers and Delaware Law" (2018) 73 The Business Lawyer 319, 331.

27 The Tokenizer, "The Security Token RegRadar Report" (*The Tokenizer*, July 2021), 57 [Oliver Völkel] <https://bit.ly/3yBR6xa> accessed 1 June 2022. For a detailed analysis, see Oliver Völkel, „Initial Coin Offerings aus kapitalmarktrechtlicher Sicht" (2017) Zeitschrift für Energie und Technikrecht 03/2017 103, 105–106.

28 Noted in 成本治男 & 岩井宏樹「アセット・トークンについて」in 堀天子 (ed.)『暗号資産の法的性質と実務』(2021) 1611 金融商事判例 104, 111 (Haruo Narimoto and Hiroki Iwai, "Regarding Asset Tokens," in Takane Hori (ed), *Legal Nature and Practice of Crypto Assets* (2021) 1611 Financial and Commercial Case Law 104, 111).

the notion of token defined as a record on a TT (trustworthy technologies) system which represents claims, membership rights or other absolute or relative rights (Article 2(1)(c)). It defines the trustworthy technologies (vertrauenswürdige Technologien: VT) in technology neutral language (Article 2(1)(a)) with the blockchain technology or DLT primarily in mind.[29] The TVTG provides that disposition of a token results in the disposition of the right represented by it (Article 7(1)). The Act also provides that the disposition of a token requires the transfer of the token, the agreement between the transferor and the transferee, and the transferor's entitlement to dispose of it (Article 6(2)). According to the Act, the holder of the TT Key, which is meant to be the private key for a blockchain-based token,[30] is presumed to be the person entitled to dispose of the token (Article 5(1)). On that basis, the Act permits *bona fide* acquisitions (*Erwerb kraft guten Glaubens*) (Article 9) and the release of obligors by *bona fide* performance (*Befreiungswirkung*) (Article 8(2)). The Act further lays down the procedure for a cancellation declaration (*Kraftloserklärung*) of tokens in case of loss of a TT Key (Article 10).

3.2.2 Swiss Law

In Switzerland, the DLT Act, examined in section 3.1.2 above, amended Article 622(1) of the Code of Obligations. The latter now provides that company shares may be issued as "ledger-based securities" if the company's articles of association so stipulate. As a result, it is now possible to issue blockchain-based shares. The provisions inserted in the Code of Obligations which concern various aspects of ledger-based securities, seen in section 3.1.2 above, would also be applicable to blockchain-based shares.

3.2.3 German Law

In Germany, the Act on Electronic Securities (Gesetz über elektronische Wertpapiere: eWpG) was enacted in 2021. For the time being, its application is limited to bearer bonds (§ 1), though it may eventually be extended to other securities.[31] It provides that securities may be issued as "electronic securities" (*elektronisches Wertpapier*) by effecting an entry in an "electronic securities register"

---

29 See section 2.5 of the Report and Application of the Government to the Parliament of the Principality of Liechtenstein Concerning the Creation of a Law on Tokens and TT Service Providers (Tokens and TT Service Provider Act; TVTG) and the Amendment of Other Laws (No. 54/2019).

30 *Id.*, 2.2.1.

31 Begründung zum Regierungsentwurf des Gesetzes zur Einführung von elektronischen Wertpapieren, BT-Drucksache 19/26925, 24.02.2021, 38 <https://dserver.bundestag.de/btd/19/269/1926925.pdf>.

(*elektronisches Wertpapierregister*) (§ 2(1)). It also provides that electronic securities generally have the same legal effect as paper securities (§ 2(1)). The concept of "electronic securities register" covers both central register (*zentrale Register*) and crypto-securities register (*Kryptowertpapierregister*) (§ 4(1)). It is further provided that a crypto-securities register must be kept on a forgery-proof recording system in which the data is logged in time sequence and saved against unauthorised deletion and subsequent changes (§ 16(1)). This provision, though using a technology-neutral expression, clearly envisages blockchains. The eWpG also contains provisions on the transfer of electronic securities (§ 25) and their *bona fide* acquisition (§ 26).

4 Emerging Choice-of-Law Rules

In the foregoing section (section 3), we have examined examples of legislation on substantive rules which give recognition to blockchain-based negotiable instruments. We will now turn our attention to choice-of-law rules.

There are hardly any tailor-made choice-of-law rules for blockchain-based negotiable instruments.[32] The Liechtenstein Token and TT Service Provider Act, examined in section 3.2.1 above, only contains what may be read as unilateral choice-of-law rules.[33] Switzerland and Germany have, however, recently

32 The proposed EU Regulation on the law applicable to the third-party effects of assignments of claims (Proposal for a Regulation of the European Parliament and of the Council on the law applicable to the third-party effects of assignments of claims, [2018] COM/2018/096 final, 2018/044 (COD)) contains, in the version amended by the Council on 28 May 2021 (Council of the European Union, "Proposal for a Regulation of the European Parliament and of the Council on the law applicable to the third-party effects of assignments of claims - General approach (9050/21)" (*CEU*, 28 May 2021) <https://data.consilium.europa.eu/doc/document/ST-9050-2021-INIT/en/pdf>), a choice-of-law rule which provides that the law applicable to the assigned claim governs the third-party effects of the assignment of "claims arising out of crypto assets." *Id.*, Article 4(2)(ba). Financial instruments and electronic money are excluded from this rule. It is not clear whether the concept "claims arising out of crypto assets" covers claims represented by crypto assets serving as blockchain-based negotiable instruments. It remains to be seen whether this proposed rule will make its way into the final text.

33 Tokens and TT Service Provider Act (n 29), Article 3(2) provides that the chapter titled "civil law foundation (Zivilrechtliche Grundlagen)" of the Act is applicable where tokens are generated or issued by a TT Service Provider having its seat or domicile in Liechtenstein or where the parties transacting tokens expressly declare its provisions to be applicable.

introduced in their legislation choice-of-law rules applicable to blockchain-based negotiable instruments. These will be examined below.

4.1 *Swiss Law*

In Switzerland, the DLT Act, examined in sections 3.1.2 and 3.2.2 above, amended the Federal Act on Private International Law (*Bundesgesetz über das Internationale Privatrecht*) with effect from 1 February 2021. The amendment inserted Article 145a, according to which whether a claim (*Forderung*) is represented by a negotiable instrument in paper or an equivalent form is determined by the law designated in the instrument or, failing such a designation, by the law of the State where the issuer has its seat or, in its absence, is habitually resident (paragraph 1). The same rules apply to documents of title to goods such as bills of lading (Article 106(1)) on the rationale that the right to claim the delivery of goods is also a claim (*Forderung*).[34] Blockchain-based bills of lading would be a negotiable instrument in a form equivalent to paper for the purpose of these rules. On the other hand, Article 145a has no application to the instruments representing company shares. It is assumed[35] that the law applicable to the company (*lex societatis*) determines whether shares can be represented by an instrument and to what extent the transfer of the instrument entails the assignment of the shares.

If the legal system specified by Article 145a(1) links the assignment of a claim to the transfer of the negotiable instrument by which it is represented, the next question that will arise is how the instrument is transferred. According to the official explanatory note for the DLT Act,[36] this question is governed by the same law as specified by Article 145a(1) if the instrument is in electronic form. If the instrument is in paper form (*physischer Titel*), that issue is subject to the law of the place where it is located (*lex cartae sitae*) (Article 145a(2) and, with respect to documents of title to goods, Article 106(2)). The Federal Council's DLT Report,[37] which laid the groundwork for the DLT Act, states that the *lex cartae sitae* principle has no application where the instrument is recorded on a distributed ledger as its situs is difficult to be envisioned.[38]

---

34 The Botschaft (n 13), 298.

35 *Id.*, 299.

36 *Id.*, 300.

37 Swiss Federal Council, "Legal framework for distributed ledger technology and blockchain in Switzerland" (*The Federal Council*, 14 December 2018) <https://www.newsd.admin.ch/newsd/message/attachments/55153.pdf> (hereafter "Federal Council's DLT Report").

38 *Id.*, para. 5.3.3.6.

The same report observes that in most cases a negotiable instrument will designate a legal system in its terms and conditions.[39] The law so designated will usually be the same as the law governing the claim represented by the instrument, though these two laws do not necessarily coincide with each other. The difference may sometimes surface where the instrument represents a claim which arises prior to the creation of the instrument. Thus, it could happen, though infrequently, that a bill of lading contains a choice-of-law clause in favour of one legal system while the contract of carriage contains a choice-of-law clause in favour of another legal system.

The law designated by a negotiable instrument will usually be the same as the law specified in the "registration agreement (Registrierungsvereinbarung)," though they may not, on a strict analysis, necessarily be the same. The Code of Obligations provides that the transfer of ledger-based securities is subject to the stipulations of the registration agreement (Art. 973f) and that the agreement must be recorded in the securities ledger or in a linked accompanying database (Art. 973d(2)). According to the official explanatory note for the DLT Act,[40] the registration agreement is an agreement to assert or transfer a right only through a tamper-resistant securities ledger. It is further explained that this agreement may be made by means of terms and conditions for the issuance of ledger-based securities.

As regards the pledging of a claim, Article 105, rather than Article 145a, is applicable.[41] The DLT Act extended the application of that Article to the blockchain-based negotiable instruments by inserting therein a provision saying that the rule for the pledging of claims (*Forderungen*) is also applicable to the pledging of other rights, provided they are represented by a book-entry security (*Wertrecht*, *droit-valeur*), a paper negotiable instrument (*Wertpapier*, *papier-valeur*) or an equivalent instrument (Article 105(2)).[42] The rule referred to in this provision states that in the absence of a choice of law by the parties,[43] the law of the place of the pledgee's habitual residence governs the pledging of claims. It is explained in a commentary that this connecting factor was adopted since a pledgee is considered to be an economically decisive person.[44]

39 *Id.*, para. 5.3.3.2.

40 The Botschaft (n 13), 276.

41 *Id.*, 300.

42 *Id.*, 297.

43 The choice of law made by the parties cannot be asserted against third parties (Article 105(1)), though third parties may accept the chosen law if it would work to their advantage: Andreas Bucher (ed), *Commentaire Romand: Loi sur le droit international privé – Convention de Lugano* (Helbing & Lichtenhahn, 2011), 854 [by Louis Gaillard].

44 *Id.*, 855.

A contrast may be made with the pledging of the other rights, which is referred to the law applicable to the right in question (Article 105(2)). According to a commentary, such other rights include the rights of authors and patents, hereditary shares, and land titles.[45] The same commentary states that the legislature considered that these other rights would not usually be pledged in bulk.[46] In contradistinction, the legislature apparently considered that rights represented by negotiable instruments would more often be pledged in bulk.

4.2 *German Law*

The Act on Electronic Securities (eWpG), examined in section 3.2.3 above, contains choice-of-law rules in § 32, which refers to the law of the State supervising the register-keeping entity (*registerführende Stelle*) in whose electronic securities register (*elektronisches Wertpapierregister*) the instrument is entered (paragraph 1). According to an official explanatory note,[47] the supervising State was chosen as the connecting factor because the general "*lex rei sitae*" principle (enshrined in Article 43(1) of the Introductory Act to the German Civil Code (*Einführungsgesetz zum Bürgerlichen Gesetzbuch*: EGBGB)), which would point to the law of the place of the certificate ("*lex cartae sitae*") if the securities were in paper form, would make no sense if the instrument is in electronic form, and also because identifying the place of an electronic register is difficult.

After specifying the primary connecting factor in paragraph 1, § 32 goes on to provide subsidiary connecting factors in paragraph 2. Thus, in the cases where the register-keeping entity is not under the supervision of any State, § 32(2) specifies the seat (*Sitz*) of the register-keeping entity as the connecting factor. Again, in the cases where the seat cannot be identified, § 32(2) specifies the seat of the issuer of the electronic securities as the connecting factor. It does not, however, offer a solution where the same register-keeping entity comes under the supervision of more than one State.

What is somewhat puzzling about these provisions is that they presuppose that there is necessarily a register-keeping entity for the electronic securities register. As noted in section 3.2.3 above, the concept of "electronic securities register" (*elektronisches Wertpapierregister*) covers both central register (*zentrale Register*) and crypto-securities register (*Kryptowertpapierregister*) (§ 4(1)). It is easy to see that there is a register-keeping entity for central registers. With respect to crypto-securities registers, the register-keeping entity is

45 *Id.*
46 *Id.*
47 Gesetzentwurf der Bundesregierung (n 31), 69.

defined as someone who is designated as such by the issuer or, failing such a designation, the issuer itself (§ 4(10) and § 16(2)). But it is also provided that the register-keeping entity must ensure that the register accurately reflects the current legal situation at all times (§ 7(2)), which seems to imply that the register-keeping entity is technically equipped to change the register at will. While that possibility may exist with private blockchains (blockchains administered by a specific entity), it would not be possible with public blockchains (blockchains for which there is no specific entity acting as administrator). It seems to follow that a crypto-securities register (*Kryptowertpapierregister*) within the meaning of this Act is necessarily a private blockchain.[48]

5 Discussion on Choice-of-Law Rules

In the foregoing sections (sections 3 and 4), we have examined the substantive rules and choice-of-law rules of some States applicable to blockchain-based negotiable instruments. We will now consider what the choice-of-law rules should be for the issues arising out of such instruments.

5.1 *Architecture of Trading and Holding*

As the choice of law analysis is an exercise of finding appropriate connecting factors to localise the issues in specific jurisdictions, it would be helpful to envision the architecture of holding and trading of blockchain-based negotiable instruments. The representation below is based on the author's understanding of the emerging architecture and prediction towards the future for the trading and holding of blockchain-based bills of lading and crypto-securities. There is, however, a great deal of murkiness in the emerging architecture and a lot of uncertainty over how it will develop.

48 For a similar comment on the draft bill, see Matthias Lehmann, "Stellungnahme zum Referentenentwurf für ein Gesetz über elektronische Wertpapiere (eWpG)" (14 September 2020), 12 <https://bit.ly/2W7iWDW>. Dominik Kloka and Georg Langheld, "Gesetz zur Einführung von elektronischen Wertpapieren beschlossen" (*Noerr Newsroom*, 10 May 2021) <https://bit.ly/3kAcNJ1>, also observes the tension with the decentralization philosophy of the blockchain technology. On the other hand, Thorsten Voß, "Der Regierungsentwurf des eWpG und das Depotrecht – Ein Warnruf" (2021) 1 Zeitschrift für das Recht der digitalen Wirtschaft 16, 18, suggests, on the assumption that public blockchains could serve as an electronic securities register, that insurance may be a solution for curbing the risk of civil liability that the register-keeping entity may incur for failing to properly maintain the register.

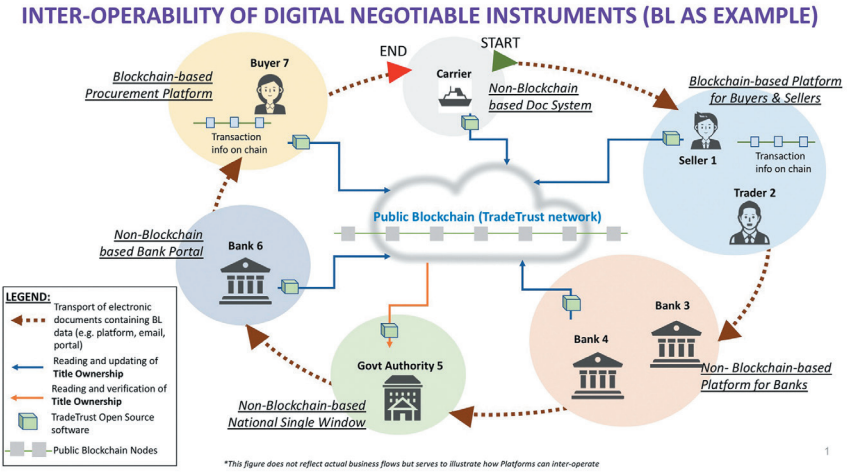

FIGURE 18.1 Inter-operability of digital negotiable instruments
SOURCE: LOH, S.Y. (2021, MARCH 31). TRADE - ADAPTING TO PRESENT AND FUTURE CHALLENGES, MARITIME TRADE DIGITALISATION – ELECTRONIC BILLS OF LADING [WEBINAR], INFOCOMM MEDIA DEVELOPMENT AUTHORITY OF SINGAPORE. HTTPS://WWW.MPA.GOV.SG/WEB/PORTAL/HOME/MARITIME-COMPANIES/RESEARCH-DEVELOPMENT/TECHNOLOGY-WEBINARS

5.1.1 Bills of Lading

Lately, projects using blockchains as a solution to digitise bills of lading have sprung up. Several among them have received approval from the International Group of P&I Clubs, an approval necessary for their insurance coverage to be extended.[49] Notwithstanding the advantage of a permissionless blockchain architecture as noted in section 3.1 above, some of these projects appear to be member-only systems. One of the models utilising a permissionless blockchain is illustrated in Figure 18.1. The center of this figure shows a public blockchain, which is necessarily permissionless since there is no specific entity to give permissions to its users. But all sensitive information could be hidden from public view, so that the details of bills of lading such as the names of the parties and the content of the cargo are transmitted outside the blockchain by means of conventional methods of communication such as emails. The interface with the blockchain may be provided by a number of commercial entities competing to offer user-friendly services.

49 The Swedish Club, "Electronic (Paperless) Trading" (*The Swedish Club*, 29 March 2021) <https://bit.ly/3kGUWQm>.

5.1.2 Crypto-securities

Financial sectors are subject to intensive regulation to safeguard the integrity of the market and to counter money laundering. A conventional regulatory approach relies on the existence of a specific entity which is supervised and held accountable. There is a view that says the involvement of regulated entities is necessary even where blockchains are used to issue and trade securities.[50] That would not, however, mean that crypto-securities may only be issued on private blockchains administered by a specific entity since there are also other actors whom the regulators may target. These include the providers of an interface with the blockchain, wallet providers, the operators of trading platforms, the issuer of crypto-securities, and the keeper of shareholder or bondholder directories.[51] Compliance with anti-money laundering rules may also be facilitated by innovations in the area of e-identity, which does not have to be granted by financial intermediaries but can be part of the e-government tools.[52] There is currently the practice of issuing crypto-securities on public blockchains[53] and this practice may continue in the future whether in the mainstream or on the fringe.

As the blockchain technology allows for disintermediation, crypto-securities may be issued directly to investors, held by them directly without relying on third party custodians, and traded peer-to-peer or on a defi (decentralised

50 Andrea Pinna and Wiebe Ruttenberg, "Distributed ledger technologies in securities post-trading – Revolution or evolution?" (2016) European Central Bank Occasional Paper Series 172, 23.

51 The directories of shareholders and bondholders may be kept in a separate database from the blockchain on which crypto-tokens are issued. That database may itself take the form of a blockchain, as acknowledged in § 81a(2) of the Final Part (Schlussabteilung) of the Liechtenstein Persons and Companies Act (Personen und Gesellschaftsrecht (PGR) vom 20. Januar 1926). It is not impossible that the same blockchain on which the cryptosecurities are issued is used as directories of shareholders and bondholders, as acknowledged by the Botschaft (n 13), 274. Whenever a blockchain is used as directories of shareholders or bondholders, it will necessarily be a private blockchain to avoid disclosing confidential information such as the identity of the holders: See Olivier Favre et al., "Trends and Developments" (*Schellenberg Wittmer Ltd*, 17 June 2021) <https://bit.ly/2VgQ77I>.

52 Pinna and Ruttenberg (n 50), 30.

53 Oliver Völkel and Bryan Hollmann, "Tokenization in Austria" (*Stadler Völkel*, 2021), 2 <https://bit.ly/2ULzXmK> states that the Ethereum blockchain, a major public blockchain, is most frequently used for the purpose of tokenization. The Bitbond, the first of regulated crypto-securities in Germany, was offered on the Stellar blockchain, another example of public blockchain (para. 7.2.1 of Bitbond, "Securities Prospectus of Bitbond Finance GmbH, Berlin" (*Bitbond*, 30 January 2019) <https://www.bitbondsto.com/files/bitbond-sto-prospectus.pdf>).

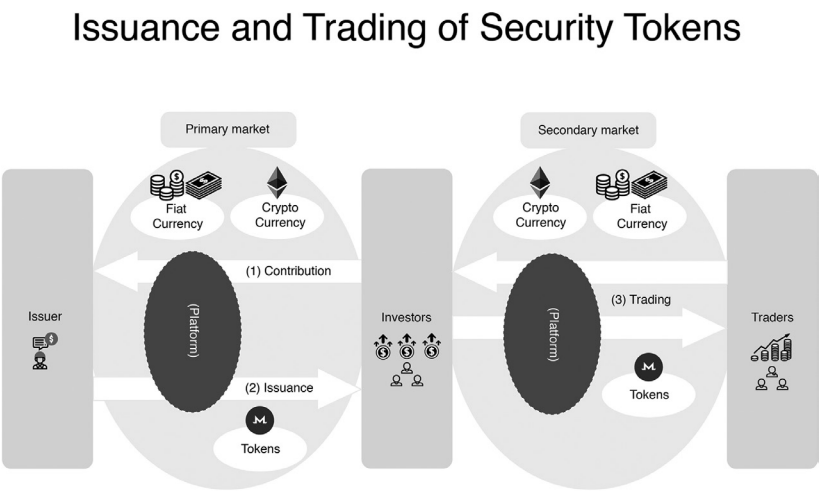

FIGURE 18.2 Issuance and trading of security tokens

finance) platform. If, however, issuers and traders wish for a high liquidity environment to issue and trade crypto assets, they may prefer using centralised platforms (see Figure 18.2). Centralised platforms include crypto-assets exchanges, traditional securities exchanges, and multilateral trading facilities. Their availability depends on the applicable regulatory regimes.

The current uncertainty over the architecture of trading and holding crypto-securities[54] is particularly acute on the side of the secondary market. Where crypto-securities are traded on a peer-to-peer basis or on a defi platform, no intermediaries would be needed (See Figure 18.3).

Where, on the other hand, a centralised trading platform is used, the architecture will vary considerably. Thus, if the crypto-securities are listed on a crypto-assets exchange or a similar trading platform, the retail investors may directly participate in trading.[55] If the crypto-securities are listed on a

54 Also acknowledged by the Proposal for the Regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology, [2020] 2020/0267 (COD), Recital (3).

55 The Swiss DLT Act introduced, with effect from 1 August 2021, a new chapter (Ch. 4a in Title 2) in the Financial Market Infrastructure Act (Bundesgesetz über die Finanzmarktinfrastrukturen und das Marktverhalten im Effekten- und Derivatehandel (Finanzmarktinfrastrukturgesetz, FinfraG) vom 19. Juni 2015, SR 958.1) to create a new license category for "DLT trading facilities" (*DLT-Handelssysteme*) which, unlike the pre-existing trading platforms licensed in Switzerland, allow retail investors to trade crypto-securities directly (Article 73c(1)(e)). For an analysis, see Manuel Meyer and Yves Mauchle, "Switzerland" (2021) Butterworths Journal of International Banking and Financial Law 157, 159.

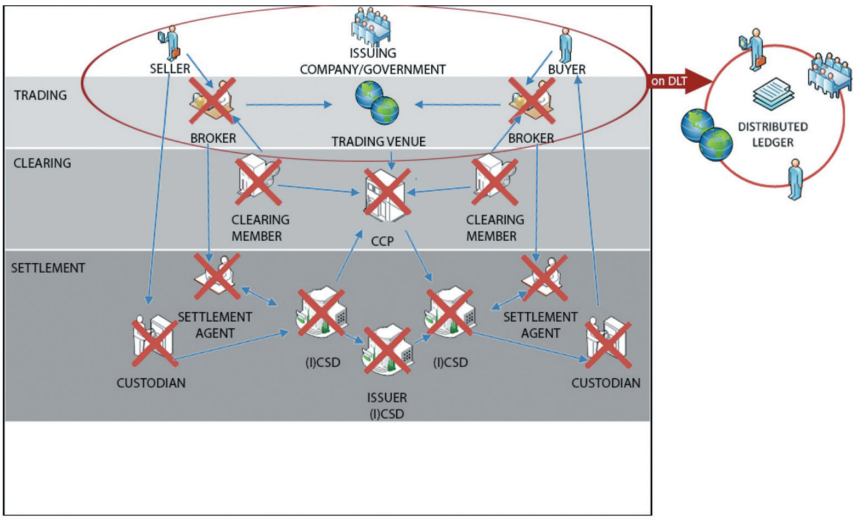

FIGURE 18.3 Trading on a distributed ledger
SOURCE: DIAGRAM 4 FROM PINNA & RUTTENBERG, "DISTRIBUTED LEDGER TECHNOLOGIES IN SECURITIES POST-TRADING" *SUPRA* NOTE 50, P. 31

traditional securities exchange or a multilateral trading facility (MTF), the retail investors may only be able to participate in trading through their brokers. Some trading platforms may dispense with intermediaries for post-trading phases (see Figure 18.4) by adopting a distributed ledger settlement process which may be combined with a smart contract functionality. In some cases, crypto-securities may be held by a central securities depository (CSD) with possibly a layer of custodians between the latter and retail investors.

5.2 *The Lineup of Issues for Choice of Law*

Blockchain-based negotiable instruments will raise a number of issues for which the governing law needs to be determined. The lineup is as sketched out below.[56]

To begin with, there are issues of creation and cancellation of a blockchain-based negotiable instrument. Most fundamentally, there is the issue of
1 whether a blockchain-based token may be created to serve as a negotiable

56 This lineup is not meant to be exhaustive. Additionally, there is, for example, the issue of what impact, if any, the rescission or termination of the underlying contract has on the assignment of the right which has been effected through the transfer of a negotiable instrument. There is also the issue, unique to a blockchain-based instrument, of what effects a hard-fork of the blockchain has on the represented right.

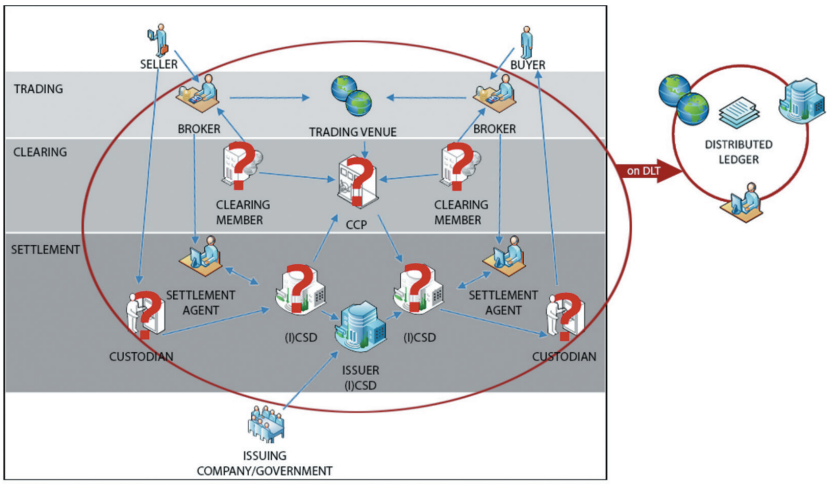

FIGURE 18.4 Post-trade clearing and settlement on a distributed ledger
SOURCE: DIAGRAM 3 FROM PINNA & RUTTENBERG, "DISTRIBUTED LEDGER TECHNOLOGIES IN SECURITIES POST-TRADING" *SUPRA* NOTE 50, P. 29

instrument to represent the right in question.[57] This issue may be understood to comprise a sequence of sub-issues: whether a negotiable instrument may be created for the right in question; whether a negotiable instrument may be in electronic form; and whether the electronic negotiable instrument may take the form of a blockchain-based token. The flip side of issue ***1*** is issue ***2***: whether a blockchain-based negotiable instrument may, in case of loss of the private key, be cancelled. Where a paper-based negotiable instrument is lost, stolen or destroyed, some legal systems provide for procedures for a cancellation declaration (*Kraftloserklärung*) of the instrument, so that the beneficiary could assert the right represented by it without the possession of it.[58] The

57 See *e.g.*, § 516(2) of the German Commercial Code (Handelsgesetzbuch), mentioned in section 3.1.1 *supra*; Article 1153a of the Swiss Code of Obligations (n 12), mentioned in section 3.1.2 *supra*; Article 2(1)(c) of the Tokens and TT Service Provider Act (n 29), mentioned in section 3.2.1 *supra*; Article 622(1) of the Swiss Code of Obligations (n 12), mentioned in section 3.2.2 *supra*; and § 2(1) of the German Act on Electronic Securities (Gesetzes zur Einführung von elektronischen Wertpapieren vom 3. Juni 2021 (BGBL. I S. 1423) ("eWpG")), mentioned in section 3.2.3 *supra*.

58 See *e.g.*, Article 973h of the Swiss Code of Obligations (n 12), mentioned in section 3.1.2 *supra*, and Article 10 of the Tokens and TT Service Provider Act (n 29), mentioned in section 3.2.1 *supra*. Such procedures do not generally exist in common law jurisdictions. With respect to the cancellation of bills of lading, see Koji Takahashi, "Judicial Decree to Terminate the Validity of Lost Bills of Lading" (2008) 39 Journal of Maritime Law & Commerce 551, 552.

issue whether such procedures are available would also arise with a blockchain-based negotiable instrument.

The legal systems which recognise blockchain-based negotiable instruments would associate with them certain effects concerning the assertion and discharge of the rights represented by them. The issues which may arise in this connection[59] include ***3*** whether, for the exercise of the right represented by such an instrument, it is necessary to become a holder of the instrument. There is also the issue ***4***: in what circumstances, if any, the obligor is discharged from its obligation by providing performance to the holder of such an instrument should it be proven that the latter is not the owner of the right represented by it.[60]

The legal systems which recognise blockchain-based negotiable instruments would also associate with them certain effects concerning the assignment of the rights represented by them. The basic issue which will arise in this connection is ***5*** what are the requisites for the right represented by such an instrument to be assigned, in particular whether it is necessary and/or sufficient for the instrument to be transferred to the assignee. Under some legal systems, the qualification of an instrument as a negotiable instrument may mean that its transfer is both necessary and sufficient to assign the right represented by it, leaving only the question of what the requisites are for the transfer of the instrument.[61] But that would not be the only conceivable model since the "representation" of a right by an instrument could have diverse implications.

---

59 These issues are excluded from the scope of the Rome I Regulation (Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), [2008] OJ L177/6 ("Rome I Regulation")) since they concern obligations arising out of the negotiable character of a negotiable instrument (*id.*, Article 1(2)(d)). Under this provision, the word "negotiable" seems to be used in a sense broader than that which describes the character of an instrument that allows a *bona fide* transferee to acquire a better title than what the transferor had. For the meaning of broader and the narrower senses, see section 1 *supra*). For a contrary view under Article 1(2)(c) of the Rome Convention (The Convention of 19 June 1980 on the Law Applicable to Contractual Obligations, [1980] OJ L/1980/266/1), see William Tetley, with the assistance of Robert C. Wilkins, *International Conflict of Laws: Common, Civil and Maritime* (Montreal: Blais 1994), 309, 311–312. In this book, it is argued that a bill of lading is not subject to the exclusion of Article 1(2)(c) because it is not a negotiable instrument in either the common law or the civil law (except under the German theory). It should be noted, however, that the Rome I Regulation (n 59) seems to acknowledge that bills of lading possess negotiable character (see Rome I Regulation (n 59), Recital (9)).

60 See *e.g.*, Article 8(2) of the Tokens and TT Service Provider Act (n 29), mentioned in section 3.2.1 *supra*.

61 See *e.g.*, *id.*, Article 6(2) mentioned in section 3.2.1 *supra*.

Another issue of particular importance is the possibility of *bona fide* acquisition, that is to say ***6*** whether and under what conditions a *bona fide* transferee of an instrument may acquire a better title than the transferor.[62]

5.3 *Solution Suggested by this Paper*

This paper suggests that the *lex creationis* should be applied to determine the issues from ***1*** to ***4***. The *lex creationis* is the law under which the right represented by the negotiable instrument is created, such as the law applicable to the underlying claim. For example, with respect to the right to claim the delivery of goods represented by a bill of lading, it is the governing law of the carriage contract.[63] With respect to the right to claim the payment of a sum of money represented by a bond,[64] it is the governing law of the bond, which would usually be specified in the prospectus. With respect to the membership right represented by a company share, it is the *lex societatis,* which would, depending on the applicable choice-of-law rules, be the law of the place of incorporation or the law of the real seat of the company.

With respect to issues ***5*** and ***6***, this paper suggests that the *lex creationis* should as a general rule be applicable in relation to all negotiable instruments (including bills of lading and investment securities) issued on a blockchain, subject to exceptions for the following two categories of cases: Firstly, where a permissioned blockchain is used to issue the negotiable instrument and there is consent to a choice-of-law clause by all its users, the law specified by the clause should prevail over the *lex creationis*. Secondly, where crypto-securities

62 See *e.g.*, § 932 of the German Civil Code (n 2), mentioned in section 3.1.1 *supra*; § 26 of the eWpG (n 57), mentioned in section 3.2.3 *supra*; Article 973e(3) of the Swiss Code of Obligations (n 12), mentioned in section 3.1.2 *supra*; and Article 9 of the Tokens and TT Service Provider Act (n 29), mentioned in section 3.2.1 *supra*.

63 As determined by Article 5 of the Rome I Regulation (n 59), if the latter is applicable. The determination of the governing law of a carriage contract is not excluded from the scope of the Regulation even where the right to claim the delivery of goods under the contract is represented by a bill of lading since that obligation does not arise out of the negotiable character of a bill of lading (See *id*., Article 1(2)(d)).

64 It includes a convertible bond until it is converted into equity: See para. 522 of UNCITRAL, "UNCITRAL Model Law on Secured Transactions: Guide to Enactment" (*UNCITRAL*, 2017) <https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/mlst_guide_to_enactment_e.pdf>. It also includes a profit participation certificate (Genussschein) which represents a profit participation right (Genussrecht), *i.e.*, the right that is granted by a corporation and limited to monetary claims (with membership rights such as voting rights being excluded) (Klaus Weber (ed), *Creifeld's Rechtswörterbuch* (26th edn., München: C.H. Beck 2021)). According to Völkel and Hollmann (n 53), 2, Genussrecht is currently the most popular right to be tokenised in Austria.

are held with an intermediary, the governing law should be determined in accordance with the existing choice-of-law rules for securities held with an intermediary. In the situations which fall within both of these two categories, the rule for the second category should take precedence.

What follows will first elucidate the meaning of "*lex creationis*" and then offer the basic reason for the solution suggested above.

5.4 *The Meaning of "lex creationis"*

Professor Ooi, a long-term proponent of applying the *lex creationis* for the proprietary aspects of securities – whether certificated or held with an intermediary – extends her proposition to crypto-securities in her latest paper.[65] Given the prominence of Professor Ooi's writings in this field of law, it is worth noting that what is meant by the *lex creationis* in her paper does not seem to be exactly identical to the same expression used in the present paper. Both papers understand the concept of *lex creationis* as referring to the law under which the object in question is created.[66] The object in question seems, however, different: while the present paper looks to the right represented by a negotiable instrument, Professor Ooi's paper appears (at least in some places) to look to the token or other medium representing the right. This is gleaned from the observation in her paper that "the law of the system" is a manifestation of the *lex creationis*.[67] The meaning of "the law of the system" is said to be different depending on the type of securities – whether certificated, intermediated, or in the form of crypto-securities. For intermediated securities, it is said to be the law of the intermediated system and for crypto-securities, it is said to be the law of the "cryptosecurities system." The latter is described as a system that allows for the crypto-securities to be created and issued within it.[68] Professor Ooi argues that the law of that system should be applicable to the proprietary aspects of crypto-securities. Whatever exactly is meant by the law of the "cryptosecurities system," it does not appear to be necessarily the same as the *lex creationis* of the right represented by crypto-securities.

---

65 Maisie Ooi, "Choice of Law in the Shifting Sands of Securities Trading," in Andrew Dickinson and Edwin Peel (eds), *A Conflict of Laws Companion* (Oxford: Oxford University Press 2021), 199.

66 *Id.*

67 *Id.*, 220.

68 *Id*. It is, however, also said elsewhere (*id.*, 219) that the law of the cryptosecurities system" is the law "with which the cryptosecurities have their most significant connection."

5.5 *The Basic Reason for the Suggestion*

As noted in section 5.3 above, this paper suggests that the *lex creationis*, the law under which the right represented by a blockchain-based negotiable instrument is created, should be applied to determine all the issues from ***1*** to ***4*** and, subject to two rules of exception, issues ***5*** and ***6***. This suggestion basically rests on the ground that all these issues concern the state-of-being (namely, creation, extinction, and all intervening dispositions such as transfers and encumbrances) of the right in question. To determine the state-of-being of a right by applying the law under which it is created is not only logical but would also usually meet the expectation of the interested parties. The point will be expounded below with respect to each of the issues from ***1*** to ***6***.

The issue ***1*** whether a blockchain-based token may be created to serve as a negotiable instrument to represent the right in question concerns the state-of-being of the right. The point might be better appreciated if the issue is re-phrased as "whether the right in question may be represented by a blockchain-based token serving the role of a negotiable instrument." So re-phrased, it would also be appreciated that the answer should be the same[69] irrespective of whether the negotiable instrument is in paper or electronic form and irrespective of whether it is recorded in a central register or distributed ledger.

Issue ***2*** should be dealt with in the same way as issue ***1*** since it is the flip side of the latter. Again, the issue concerns the state-of-being of the represented right. With respect to a paper-based bill of lading which is lost, stolen or destroyed, a leading scholarly opinion in Japan favours the application of the law of the country in which the port of discharge is situated to determine the issue corresponding to ***2***.[70] This opinion is based on the idea that the way in which a right may be asserted is closely connected to the law of the place where it is to be asserted. Another scholarly opinion favours the application of the law governing the carriage contract on the ground that how the loss of a bill of lading may be remedied is a question that affects the right against the carrier in terms of how it may be asserted.[71] The latter opinion accords with this paper's suggestion in both conclusion and reasoning.

---

69 A leading scholarly opinion in Japan with respect to paper-based bills of lading also favours the application of the law governing the contract of carriage (noted in 佐野寛『国際取引法』(Hiroshi Sano, *International Trade Law* (4th edn, Yuhikaku 2014), 157).

70 As noted in Takahashi (n 58), 560, though this opinion is not shared by the author.

71 As noted in 高橋宏司「船荷証券の除権決定のための公示催告手続の国際裁判管轄」(Koji Takahashi, "Jurisidiction to Issue a Decree Terminating the Validity of Lost Bills of Lading" (2008) 199 Kaijiho Kenkyu Kaishi 2, 5).

Issues ***3*** and ***4*** pertain to the assertion and discharge of the right represented by a blockchain-based negotiable instrument and, accordingly, concern the state-of-being of that right.

Likewise, issues ***5*** and ***6*** pertain to the assignment of the represented right and, again, concern the state-of-being of that right. Since any purported assignment of the same right outside the blockchain may, depending on the applicable choice-of-law rules, also be subject to the *lex creationis*, a divergence between on-chain and off-chain transactions may be avoided.

Issues ***5*** and ***6*** pertaining to the assignment of the represented right should be distinguished from the question what effect, if any, bills of lading have on the disposition of real rights in the goods. Bills of lading represent the right to claim the delivery of goods under a contract of carriage, rather than real rights in the goods.[72] Nonetheless, the applicable law may associate with them certain effects concerning real rights in the goods.[73] Thus, the transfer of a bill of lading may have the effect of passing property in goods under some legal systems.[74] Under other legal systems, the transfer of a bill of lading perfects the passing of property in goods by conferring on the transferee an *erga omnes* title, a title which can be asserted against all persons.[75] The issue of what effect, if any, bills of lading have on the disposition of real rights in goods concerns the state-of-being of the real rights and should be determined by the *lex situs* of the goods, regardless of the medium of the bills of lading.[76]

---

72 Also noted in the Federal Council's DLT Report (n 37), para. 5.3.3.4 (fn. 343).

73 *Id*.

74 The repealed English Bills of Lading Act 1855 (1855 c. 111) stated in the opening of section 1 that "[e]very Consignee of Goods named in a Bill of Lading, and every Endorsee of a Bill of Lading to whom the Property in the Goods therein mentioned shall pass, upon or *by reason of* such Consignment or Endorsement" (emphasis supplied).

75 As is the position under Japanese law by virtue of the combined effect of Article 178 of the Japanese Civil Code (n 2) and Article 763 of the Japanese Commercial Code (Act No. 48 of 9 March 1899). The former provides that the passing of property in movable goods may not be asserted against third parties unless the goods have been delivered to the transferee. The latter provides that the delivery of a bill of lading to its lawful holder has the same legal effect as the delivery of the goods represented by it.

76 For the same view in the context of paper-based bills of lading, see *e.g.*, 嶋拓哉「物的権利関係の準拠法と運送証券の発行」 (Takuya Shima, "The Law Applicable to Real Rights and the Issuance of Documents of Title to Goods" (2014) 64 Hokkaido University Law Review 1, 38). The Federal Act on Private International Law of Switzerland ("PILA") provides that if several persons assert a real right in goods, some directly, others on the basis of a title document, the law applicable to the goods themselves determines whose right prevails (Federal Act on Private International Law (PILA) of 18 December 1987, SR 291, Article 106(3)).

5.6 *Considerations Relevant Only to Issues 5 and 6*

This paper's suggestion that the *lex creationis* should be applicable would not be so controversial with respect to issues ***1*** to ***4***. There is, however, more room for disagreement with its suggestion for issues ***5*** and ***6*** that, as a general rule, the *lex creationis* should be applicable. It is because there are considerations, other than the state-of-being of the right argument, which are relevant to issues ***5*** and ***6***. Focusing on these issues,[77] the following analysis will examine three of these considerations.

5.6.1 Whether the Lex Rei Sitae Principle Should Be Followed

Where the negotiable instrument is in paper form, a conventional view would apply the law of the place where the instrument is situated (*lex cartae sitae*), rather than the *lex creationis* of the represented right, to determine the issues corresponding to ***5*** and ***6***.[78] The *lex cartae sitae* is a manifestation of the *lex rei sitae* principle, a principle whereby the property aspects of an asset are to be decided by the law of the place where the asset is situated. The latter is a well-established principle for tangible assets and is justified for promoting legal certainty since the location of a tangible asset is easily ascertainable. As the right represented by a negotiable instrument is not tangible, the conventional view may be understood as fictionally treating the location of the negotiable instrument as the situs of the represented right. Since the economic value of a negotiable instrument, being a mere piece of paper, is miniscule, it would make no practical sense to treat a negotiable instrument itself as an object of assignment. Practically, the transfer of a negotiable instrument is only meaningful if it has some effects concerning the assignment of the represented right.

---

77 Making a separate treatment of these issues would not be unconventional in the choice-of-law analysis for paper-based securities, as may be observed in the distinction of the Wertpapiersachstatut (the law applicable to the real right aspects of a negotiable instrument) from the Wertpapierrechtsstatut (the law applicable to the rights represented by a negotiable instrument). For this distinction, see *e.g.*, Stefan Grundmann and Moritz Renner (eds), *Bankvertragsrecht 2: Commercial Banking: Zahlungs- und Kreditgeschäft* (5th edn, De Gruyter 2014), 482 [Renner].

78 See *e.g.*, Louis d'Avout, "Property and Proprietary Rights," in Jürgen Basedow et al. (eds), *Encyclopedia of Private International Law* (Edward Elgar 2017), 1429 at para. III.1.(c), which makes an observation on the basis of an examination of national laws that the *lex creationis* governs the technique of transferring an asset and where that law provides for a document permitting transfer, the *lex situs* of the document governs the transfer. See also Article 106(2) of the Swiss PILA (n 76) as well as the Botschaft (n 13), 300 on Article 145a of the same Act (examined in section 4.1 *supra*), para. (2) of which is only applicable to paper instruments. A leading scholarly opinion in Japan with respect to paper-based bills of lading also favours the *lex cartae sitae* (noted by Sano (n 69), 157).

This conventional view may be defended as promoting legal certainty as long as the location of the negotiable instrument is easily ascertainable. That is the case where the negotiable instrument is in paper form and held directly by the beneficiary.[79] The conventional view is harder to be defended where the negotiable instrument is in electronic form.[80] Where the electronic negotiable instrument is recorded in a central register, it might still be possible to resort to another fiction of treating the location of the register as the situs of the instrument. Such a fiction, however, would not work with blockchain-based negotiable instruments as they are recorded in distributed ledgers for which there is no single location.[81] It seems, therefore, appropriate to abandon the *lex rei sitae* principle where the negotiable instrument is issued on a blockchain.

5.6.2 Whether a Bulk Assignment Should Be Facilitated

Investment securities may be assigned in bulk since they are, unlike documents of title to goods, fungible. This raises the question whether the choice-of-law rules for crypto-securities should facilitate a bulk assignment, namely the assignment of a diverse portfolio of securities.

The application of the *lex creationis* would undermine the efficiency of a bulk assignment. It would impose a significant burden on the assignee, who would have to check and comply with the law governing each of the securities comprising the portfolio. It would even make it practically impossible to pledge a pool of securities which changes composition over time. There is a view that criticises the *lex creationis* rule for this reason.[82] There is even an argument that says the application of different laws to a diverse portfolio would undo much of the benefit of the blockchain technology.[83] And there is a call for a choice-of-law approach that specifies a single law to govern the entire portfolio

79 As securities certificates become immobilised and centralised with the development of the intermediate holding system, it has become less easy to ascertain their location.

80 The Japanese Commercial Code (n 75) used to contain a provision (Article 483), which provided that certain other provisions of the same Code were applicable to the transfer taking place in Japan of the shares and bonds issued by a foreign company. This provision, though not being a choice-of-law rule *per se*, could be seen as manifesting the notion that the *lex cartae sitae* should be the applicable law. It was repealed in 2004 by a law reform to facilitate the digitization of securities.

81 As examined in sections 4.1 and 4.2 *supra*, similar observations have influenced the Swiss and German legislature in devising their choice-of-law solutions.

82 嶋拓哉「抵触法の観点からみたペーパーレス証券決済」(Takuya Shima, "Paperless Securities Settlement from the Perspectives of Conflict of Laws," in 千葉恵美子 (*ed.*)『キャッシュレス決済と法規整』(Emiko Chiba (ed), *Cashless Payment and Regulations* (Minjuhô Kenkyûkai 2019), 414, 435).

83 Philipp Paech, "Securities, Intermediation and the Blockchain – An Inevitable Choice between Liquidity and Legal Certainty?" (2016) 21 Uniform Law Review 612, 636.

of crypto-securities.[84] One such choice-of-law rule would be to apply the law of the place where the assignor is habitually resident or has its seat. This connecting factor would, however, encounter difficulties where there is a chain of assignments.[85] An alternative choice-of-law rule would be to apply the law of the place where the assignee is habitually resident or has its seat. As examined in section 4.1 above, a similar rule is adopted by Article 105(2) of the Federal Act on Private International Law of Switzerland, though it is only concerned with an assignment by way of pledging as opposed to an outright transfer.

There is, on the other hand, a view that casts doubt on whether the need to facilitate a bulk assignment is relevant to crypto-securities.[86] Which viewpoint is right? The works of the UNCITRAL seem instructive. The Model Law on Secured Transactions (2016) provides as a general rule that the law applicable to the creation and effects of a security right in an intangible asset is the law of the State in which the grantor is located (Article 86).[87] For non-intermediated securities, however, the Model Law provides for exceptions to the general rule. Thus, the law applicable to the creation and effects of a security right in non-intermediated equity securities is the law under which the issuer is constituted (Article 100(1)) and the law applicable to the creation and effect of a security right in non-intermediated debt securities is the law governing the securities (Article 100(2)). These rules accordingly designate the *lex creationis* of the rights represented by the non-intermediated securities.[88] Their rationale is to be found in an earlier work of the UNCITRAL, the Legislative Guide on Secured Transactions (2007). This guide states[89] that where it is customary to conduct due diligence on each receivable to be assigned, a choice-of-law rule applying the law governing the receivable would work well while that rule would raise

84 Mark Kalderon, Ferdisha Snagg, and Claire Harrop, "Distributed ledgers: A Future in Financial Services?" (2016) 31 Journal of International Banking Law and Regulation 243, 248.

85 Financial Markets Law Committee, "Distributed Ledger Technology and Governing Law: Issues of Legal Uncertainty" (*FMLC*, March 2018), para. 6.22 <http://fmlc.org/wp-content/uploads/2018/05/dlt_paper.pdf> ("FMLC Report"). For this criticism as it applies to the assignment of receivables outside the context of negotiable instruments, see Trevor C. Hartley, "Choice of Law Regarding the Voluntary Assignment of Contractual Obligations under the Rome I Regulation" (2011) 60 International and Comparative Law Quarterly 29, 55.

86 The FMLC Report (n 85). It does not give reasons beyond mentioning the DLT environment.

87 This rule is also consistent with Articles 22 and 30 of the United Nations Convention on the Assignment of Receivables in International Trade (New York, 2001), 12 December 2001.

88 Equity securities are shares and the debt securities include bonds: UNCITRAL, *Guide to Enactment* (n 64), para. 519.

89 UNCITRAL, "UNCITRAL Legislative Guide on Secured Transactions" (*UNCITRAL*, 2010), 394 <https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/09-82670_ebook-guide_09-04-10english.pdf> accessed 1 June 2022.

difficulties in a bulk assignment where due diligence on each receivable would be either too costly or impossible. It may be inferred from this statement that the provisions of Article 100 of the Model Law are based on the presumption that where non-intermediated securities are assigned, a bulk assignment is not customary. Unless and until a contrary trading practice develops, it seems prudent to also adopt this presumption for crypto-securities[90] and allow due diligence to be conducted on each of the securities involved on the basis of the *lex creationis*. Since Article 100 makes no distinction between certificated and uncertificated securities,[91] it may, on a literal interpretation, be read to cover crypto-securities,[92] except where they are held with an intermediary.[93] A separate consideration applies where crypto-securities are held with an intermediary. As detailed later in section 5.7.2, this paper suggests a rule of exception for that category of cases.

5.6.3 Whether a Divergence with Intrinsic Tokens Should Be Avoided

As stated in section 1 above, this paper does not deal with intrinsic tokens (namely, tokens of self-anchored value) such as cryptocurrencies since they do not represent any relative rights. But they do give rise to issues pertaining to assignment,[94] which correspond to issues ***5*** and ***6***. This may lead one to think that the choice-of-law rules for these two types of tokens should be aligned.[95] From this point of view, there is a criticism of the choice-of-law rule applying

90 It must be acknowledged that this position is contrary to the idea presumably underpinning Article 105(2) of the Swiss PILA (n 76), examined in section 4.1 *supra*.

91 UNCITRAL, *Guide to Enactment* (n 64), para. 515.

92 Koji Takahashi, "Implications of Blockchain Technology for the UNCITRAL Works," in the United Nations Commission on International Trade Law (ed), *Modernizing International Trade Law to Support Innovation and Sustainable Development* (United Nations 2017), 81, 87.

93 Intermediated securities are excluded from the scope of the Model Law (Article 1(3)(c)) for the reason that the choice-of-law question is treated by the Hague Securities Convention (the Convention of 5 July 2006 on the Law Applicable to Certain Rights in Respect of Securities held with an Intermediary): UNCITRAL, *Guide to Enactment* (n 64), para. 26.

94 For an analysis on substantive rules on these issues, see *e.g.*, Koji Takahashi, "Cryptocurrencies Entrusted to an Exchange Provider: Shielded from the Provider's Bankruptcy?" in Charl Hugo (ed), *Annual Banking Law Update 2018: Recent Legal Developments of Special Interest to Banks* (JUTA 2018), 1, 6.

95 For an analysis on that assumption, see *e.g.*, 森下哲朗「仮想通貨に関する国際的な法的問題に関する考察」金融法務研究会『仮想通貨に関する私法上・監督法上の諸問題の検討』(2019) pp. 53, 76 (Tetsuo Morishita, "Consideration of International Legal Issues on Virtual Currencies," in Financial Law Study Group, *Examination of Problems in Private Law and Supervision Law Regarding Virtual Currencies* (2019) 53, 76). For a contrary view, see Ooi (n 65), 212.

the *lex creationis* for creating a divergence with intrinsic tokens.[96] No matter what choice-of-law rules are adopted for intrinsic tokens, the *lex creationis* rule would create a divergence for the simple reason that the *lex creationis* of the represented right cannot be envisaged for intrinsic tokens.

It seems, however, possible to defend the *lex creationis* rule since, despite the apparent similarity, there is a significant difference between the issues raised by these two types of tokens. Unlike the issues raised by intrinsic tokens which concern the assignment of the tokens themselves, the issues raised by tokens serving the role of a negotiable instrument concern the assignment of the represented right. The transfer of a negotiable instrument is only the means to assign the right. Since the gravity of the issues is centered on the state-of-being of the represented right, the application of the *lex creationis* seems defensible.

5.7 *The Rules of Exception for Issues 5 and 6*

The preceding analysis has offered the basic reason for the *lex creationis* rule in relation to all the issues from ***1*** to ***6*** (in section 5.5 above) and sought to defend it from possible criticisms in the context of issues ***5*** and ***6*** (in section 5.6 above). As noted in section 5.3 above, this paper suggests making exceptions to the *lex creationis* rule for issues ***5*** and ***6*** in the following two categories of cases. Firstly, where a permissioned blockchain is used to issue a negotiable instrument and there is consent to a choice-of-law clause by all its users, the law specified by the clause should prevail over the *lex creationis*. Secondly, where crypto-securities are held with an intermediary,[97] the governing law should be determined in accordance with the existing choice-of-law rules for securities held with an intermediary. In the situations which fall within both of these two categories, it is suggested that the rule for the second category should take precedence.

Another possible idea is to make a third rule of exception which, for the category of cases where crypto-securities are traded on a centralised platform, refers to the law of the jurisdiction regulating the platform. This rule would promote legal certainty since traders using a centralised platform should usually be aware of the the regulatory regime of the platform. Whether the

96 See *e.g.*, Shima (n 82).

97 Where the crypto-securities are listed and traded on a crypto-assets exchange, the provider of the exchange is not an intermediary in this sense since the retail investors may directly participate in trading (see the text accompanying (n 55)). Where, on the other hand, the crypto-securities are listed on a traditional securities exchange or a multilateral trading facility (MTF), the retail investors may only be able to participate in trading through their brokers. Whether the provider of a crypto-assets exchange may act as a broker will depend on the applicable regulatory regime. If it does, it is an intermediary within the meaning of the present discussion.

introduction of this rule is warranted depends, however, on how the architecture of trading will develop and in particular whether any of the situations coming under this category falls outside the second category. What follows will elaborate on the rules of exception for the first and second categories.

5.7.1 Where a Permissioned Blockchain is Used and There is Consent to a Choice-of-Law Clause by all Its Users

Where a private blockchain is used to issue a negotiable instrument,[98] there is a specific entity acting as its administrator. The administrator may make the blockchain "closed" by requiring anyone wishing to use it to obtain its permission. In granting permission, the administrator may require all users to give their consent to the terms and conditions it has fixed. In the terms and conditions, the administrator may include a choice-of-law clause. If such a clause may be construed as addressing issues ***5*** and ***6***, it should be given effect[99] since it would foster legal certainty more than the application of the *lex creationis* does. To that extent, the general choice-of-law rule in favour of the *lex creationis* should be replaced.

Some of the proponents who support giving effect to such a choice-of-law clause argue that the freedom of choice should be restricted.[100] Seeing the danger that an uninhibited choice of law might be used to avoid regulatory rules, it is argued that the chosen law should be approved by regulators or alternatively that the choice of a legal system having no connection to the DLT enterprise should not be permitted.[101] The need for restriction on the freedom of choice seems, however, doubtful since the law applicable to issues ***5*** and ***6*** should have no bearing on the application of regulatory rules (such as the rules imposing licensing or registration requirements on the issuance of crypto-securities or the brokering of their trading). The process of determining the applicable regulatory rules[102] is quite different from the choice-of-law rules for private-law issues.

In many cases, even where a private blockchain is used, there will be no choice-of-law clause addressing issues ***5*** and ***6***. Thus, there may be no terms

98 Concerning the question whether the blockchain on which crypto-securities are issued must necessarily be a private blockchain, see a brief discussion in section 5.1.2 *supra*.

99 See also the FMLC Report (n 85), paras. 6.5 and 6.7; Paech (n 83), 636; Morishita (n 95), 77; Shima (n 82), 435.

100 See *e.g.*, the FMLC Report (n 85), paras. 6.8 and 6.9; Morishita (n 95), 78; Shima (n 82), 434.

101 The FMLC Report (n 85), paras. 6.8 and 6.9.

102 For an analysis, see Koji Takahashi, "Prescriptive Jurisdiction in Securities Regulations: Transformation from the ICO (Initial Coin Offering) to the STO (Security Token Offering) and the IEO (Initial Exchange Offering)" (2020) 45 Ilkam Law Review 31, 33.

and conditions fixed for using the blockchain. Even if there are, these may not contain a choice-of-law clause. Even if there is a choice-of-law clause, it may be construed as only addressing contractual issues on the use of the blockchain. In light of this, it might be thought that the rule of exception to the *lex creationis* rule should be broader and cover all cases where private blockchains are used to issue negotiable instruments. Since private blockchains are invariably administered, such a choice-of-law rule might rely on a connecting factor defined by reference to the administrator. For example, it might specify the law of the place where the administrator is habitually resident or has its seat. Alternatively, it might specify the law of the jurisdiction supervising the administrator.

A difficulty such choice-of-law rules may encounter is the identification of a single administrator. The governance of blockchains varies considerably. Many are operated by a consortium of entities who share the role of administration or divide it among themselves. A connecting factor which relies on a single administrator would not work with such blockchains.[103] And it may not be always clear in the eyes of the users of the blockchain whether it is administered by a single entity or operated by a consortium of entities. Even where a single administrator is identified, a choice-of-law rule specifying the law of the place where the administrator is habitually resident or has its seat would be difficult to apply if the administrator operates from multiple places. A choice-of-law rule specifying the law of the jurisdiction supervising the administrator would be unworkable where the administrator comes under the supervision of more than one jurisdiction.[104]

For these reasons, it may be said that the *lex creationis* rule is superior, in terms of transparency, to any choice-of-law rules which rely on a connecting factor defined on the basis of the administrator of a private blockchain. It follows that the exception to the *lex creationis* rule should be limited to the cases where the negotiable instrument is issued on a permissioned blockchain with its terms and conditions including a choice-of-law clause for issues ***5*** and ***6***.

5.7.2 Where Crypto-Securities Are Held with an Intermediary

It is possible that in some cases crypto-securities are held with an intermediary. They may be held, for example, by a central securities depository (CSD) possibly with a layer of custodians between the latter and retail investors. What other situations fall within this category of cases depends on how the

103 For a similar view, see the FMLC Report (n 85), 6.17.

104 As noted in section 4.2 *supra* in relation to a similar choice-of-law rule (§ 32(1)) contained in the eWpG (n 57).

architecture of holding and trading crypto-securities will develop. There is a view that says crypto-securities in this category of cases should be subject to the same choice-of-law rules as exist today for securities held with an intermediary.[105]

The existing choice-of-law rules for intermediated securities are not internationally unified. There is a divide between, on the one hand, the instruments of the European Union which specify the applicable law by reference to the place of the relevant account[106] and, on the other, the Hague Securities Convention[107] which follows the contractual PRIMA (Place of the Relevant Intermediary Approach) (Art. 4). These approaches are subject to their own share of criticisms. Thus, against the EU approach, it is noted that legal certainty is lacking with the localization of the relevant account[108] especially where a multinational intermediary is involved. The account-by-account approach of the Hague Convention is criticised for giving rise to the so-called double interests problem.[109] Notwithstanding these criticisms and the lack of international uniformity, should the existing choice-of-law rules be extended by analogy to crypto-securities held with an intermediary? To address this question, the following considerations also seem material.

As noted in section 3.2 above, one of the advantages of the blockchain technology lies in its capability to create a direct link between the issuer and the holder of securities. This advantage would be fortified by the application of the *lex creationis* since it would allow the issuer to ascertain the owner of crypto-securities with relative ease. That advantage is, however, forsaken where the crypto-securities are held with an intermediary: under some legal

105 See *e.g.*, Christiane Wendehorst, "Digitalgüter im Internationalen Privatrecht" (2020) Praxis des Internationalen Privat- und Verfahrensrechts 490, 497; Shima (n 82), 435.

106 Article 9(2) of the Settlement Finality Directive (Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems, [1998] OJ L166/45), Article 24 of the Winding-up Directive (Directive 2001/24/EC of the European Parliament and of the Council of 4 April 2001 on the reorganisation and winding up of credit institutions, [2001] OJ L125/15), and Article 9(1) of the Financial Collateral Directive (Directive 2002/47/EC of the European Parliament and of the Council of 6 June 2002 on financial collateral arrangements, [2002] OJ L168/43).

107 At the time of writing (August 2021), there are only few contracting States. But these include influential States like the United States and Switzerland.

108 See *e.g.*, Paech (n 83), 623. See also the European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the applicable law to the proprietary effects of transactions in securities," (COM/2018/089 final), para. 3.1.

109 See *e.g.*, Maisie Ooi, "The Hague Securities Convention: a critical reading of the road map" (2005) Lloyd's Maritime and Commercial Law Quarterly 467, 484.

systems, the investor's recourse in the intermediated system primarily lies with a claim against its immediate intermediary rather than the exercise of the right represented by the securities against the issuer. This means that the argument for applying the *lex creationis* is so much the weaker. Furthermore, it should be recalled that while the *lex creationis* rule represents an approach that looks through the tiers of intermediaries to the level of the issuer, that approach was rejected by the drafters of the Hague Securities Convention[110] because of the frequency of portfolio transactions which is observed with securities held with an intermediary. The same consideration would be relevant to crypto-securities held with an intermediary. Additionally, one may note that where crypto-securities and traditional securities are held by the same intermediary, the application of the same law would have the advantage of simplicity.[111]

Although the relevant considerations seen in the above paragraphs pull in opposite directions, it may be concluded on balance that the existing choice-of-law rules for securities held with an intermediary should be extended by analogy to crypto-securities held with an intermediary.

6 Final Remarks

This paper has considered a solution for the choice-of-law issues arising from blockchain-based negotiable instruments, in particular the issues from ***1*** to ***6*** listed in section 5.2 above. It has suggested in section 5.3 above that the *lex creationis* of the right represented by the instrument should be applied to issues ***1*** to ***4***. With respect to issues ***5*** and ***6***, which concern the assignment of the represented right, the *lex creationis* should also be applicable as a general rule albeit subject to the two rules of exception as detailed in section 5.7 above.

The relative importance of the rules of exception will depend on how the trading practice will develop in the future. If, for example, the use of permissioned blockchains with a choice-of-law clause in their terms and conditions grows, the rule of exception for that category will commensurately grow in its importance.

The solution suggested by this paper may also need to be revised depending on how the practice and architecture of trading will develop. If, for example, a bulk assignment becomes an important practice for non-intermediated crypto-securities to such an extent that it is no longer customary to conduct due diligence on each of the crypto-securities to be assigned, the argument

110 Goode et al. (n 24), para. Int-38.

111 Wendehorst (n 105), 490, 497.

for choice-of-law rules facilitating a bulk assignment will earn more strength.[112] Again, depending on how the architecture of trading will develop, it may become warranted to introduce a third rule of exception applying the law of the jurisdiction regulating the centralised trading platform.[113]

The blockchain technology has made it possible to emulate paper-based negotiable instruments in an electronic environment. As tokens serving the role of negotiable instruments lay the foundation for a vital aspect of the token economy, it is one of the most promising areas of application of the blockchain technology. For that kind of economy to fly, it is essential to have a good legal infrastructure in terms of both substantive rules and choice-of-law rules. As of the time of writing (August 2021), it is still early days and the available legal materials are scarce. Hopefully, the analysis presented by this paper, though partly tentative due to the nascent state of market development, will stimulate further debate in this important area of law.

---

112 See section 5.6.2 *supra*.

113 See section 5.7 *supra*.

CHAPTER 19

Conflict of Laws and the Use of Distributed Ledger Technology in Derivatives Markets

Gregory Chartier

1 Introduction

In recent years there has been increasing interest amongst derivative market practitioners in the potential use of new technologies to optimise derivative markets, with a particular focus on the use of smart contracts and distributed ledger technology ("**DLT**").

In this chapter we address the potential use of DLT with respect to over-the-counter ("**OTC**") derivatives transactions and the relevant legal issues to be considered in respect of the use of DLT. We examine the relevant issues from an English law perspective as well as potential cross-border conflict-of-laws issues that may arise from the use of DLT. We also consider how the law could be developed so as to provide greater legal certainty regarding the applicable governing law for more complex uses of DLT with derivatives transactions.

2 DLT Systems

There is no single definition of a DLT system and multiple different forms of system are in use. The core feature, however, is the use of a distributed ledger providing an electronic record of transactions which is shared (or "distributed") amongst a network of participants (commonly referred to as "nodes"), with each copy of such electronic record being identical.

One key distinction regarding the DLT systems that are in use is between public systems and private systems. A "public" system is open to all and anyone can participate in, and see the data on, the system. A "private" system is not open to the public and can only be accessed by the permitted participants in the system.

Whilst many of the most well-known distributed ledgers (including the Bitcoin ledger) are public, it is more likely that private DLT systems will be used for transactions on the financial markets (such as derivative transactions). Where a public system is used, it may not be possible for a participant

© GREGORY CHARTIER, 2023 | DOI:10.1163/9789004514850_021
This is an open access chapter distributed under the terms of the CC BY-NC-ND 4.0 license.

to identify the true identity of its counterparty. This will be problematic for any regulated entity which, as a result, may not be able to satisfy its internal and regulatory requirements in respect of "know your customer" and anti-money laundering laws and other similar rules. It may also be difficult for a participant to verify that its counterparty has the capacity to enter into the relevant transaction, which would be exacerbated by the fact that a counterparty might be established anywhere in the world. These issues can be specifically addressed, and are therefore less likely to arise, with a private system.

In the remainder of this chapter we consider the potential use cases for DLT systems in relation to derivatives transactions and the potential legal issues that may arise under English and Private International Law ("**PIL**").

2.1 *Types of Derivative Transactions*

In this chapter we focus on OTC derivatives rather than cleared or exchange-traded derivatives. References to "derivatives" should be understood accordingly. OTC derivatives are predominantly entered into under the 1992 or 2002 forms of the ISDA Master Agreement published by the International Swaps and Derivatives Association ("**ISDA**"), which are drafted on the basis that they will be governed by either English or New York law. In 2018, ISDA also published French and Irish-law versions of the ISDA Master Agreement. However, the original versions (governed by English and New York law) remain the versions of the ISDA Master Agreement that are most used in the market. Accordingly, in this chapter, we predominantly focus on the use of English law and New York law agreements (as well as general PIL considerations).

An ISDA Master Agreement is a master netting agreement under which a broad range of derivative transactions may be entered into. It may be collateralised or uncollateralised, and we will consider the different legal and PIL issues that may arise from the use of DLT with both collateralised and uncollateralised transactions. For the purposes of this chapter, we will not consider any specificities arising from the different types of transactions that may be entered into under an ISDA Master Agreement.

2.2 *Use of DLT with an Uncollateralised Transaction*

If parties wish to enter into a derivative transaction on an uncollateralised basis, this is likely to be documented by the parties agreeing to the terms and entering into an ISDA Master Agreement (which will set out the legal framework of the relationship between them) and then agreeing and entering into a confirmation to document the terms of the particular transaction (such as an interest rate swap transaction).

There are two main ways in which such parties may seek to use DLT to assist with such a transaction. Firstly, a DLT system could be used to serve a record-keeping function in respect of the terms of the parties' transaction and documentation, as well as in respect of transaction events that occur after an agreement has been entered into (such as recording payments). As a result, rather than the parties maintaining such records in their own separate systems (which may lead to discrepancies in the parties' separate records and the potential for a dispute), all such information would be recorded on a distributed ledger resulting in the parties having identical records. Where a DLT system simply serves a record-keeping function, this is sometimes referred to as a "light chain."[1]

A more complex use of a DLT system may involve the automation of payments on the system in accordance with the terms of the transaction, resulting in the scheduled payment obligations under the transaction functioning as a smart contract. Such use of a DLT system is sometimes referred to as a 'heavy chain'.[2]

We consider some of the issues that may arise from such use cases below.

2.3 *Governing Law and Jurisdiction*

In respect of the use cases identified above, notwithstanding the use of a DLT system to assist with certain aspects of the transaction, the parties will still have entered into written legal agreements (*i.e.* an ISDA Master Agreement and a confirmation for the specific transaction) setting out the terms of the agreement between them. It is not expected in the short term that parties will enter into derivative transactions using DLT systems without also entering into such an off-ledger ISDA Master Agreement (or an equivalent local law derivatives master agreement such as a German law *Rahmenvertrag*).

The ISDA Master Agreement that the parties have entered into will specify the governing law of the agreement and the transactions entered into thereunder (for example English law). It will also specify the courts that will have jurisdiction to resolve any disputes in relation to the agreement and such transactions. The standard form English law ISDA Master Agreements contain jurisdiction clauses which provide for the English courts to have non-exclusive jurisdiction, save for certain exceptions which provide for exclusive jurisdiction

1 See, for example, ISDA, "Legal Guidelines for Smart Derivatives Contracts: Introduction" (*ISDA*, 30 January 2019), 8 <https://www.isda.org/2019/01/30/legal-guidelines-for-smart-derivatives-contracts-introduction/> accessed 28 June 2023.

2 *Id.*

in some scenarios. However, this is sometimes replaced with an exclusive jurisdiction clause in favour of the English courts. The standard form New York law ISDA Master Agreements contain jurisdiction clauses which provide for the courts of the State of New York and the United States District Court, located in the Borough of Manhattan in New York City, to have non-exclusive jurisdiction.

Parties also sometimes replace the jurisdiction provision of the ISDA Master Agreement with an arbitration agreement. This is usually only the case however where there is a doubt whether the jurisdiction in which one of the parties is located would enforce a judgment of the English or New York courts (as applicable) but such jurisdiction is a party to the Convention on the Recognition and Enforcement of Foreign Arbitral Awards, commonly known as the New York Convention, meaning an arbitral award should be enforceable in such jurisdiction. As the standard and most common approach is to include a jurisdiction clause rather than an arbitration provision in an ISDA Master Agreement, we do not address arbitration in the remainder of this chapter.

In addition to any dispute that may arise between the parties themselves in relation to a derivative transaction entered into on a DLT system, it is possible that one or both parties may seek to make a claim against an entity responsible in some respect for the provision of the DLT system. For example, there might be a claim against a software provider where a fault with the software results in a party to the derivative transaction suffering a loss.

2.3.1 Governing Law

If the parties to a derivative transaction have entered into an ISDA Master Agreement and specified English or New York law as the governing law of that agreement (and the transactions entered into thereunder, which form a single agreement in accordance with the terms of the ISDA Master Agreement) then, in the event of a dispute, the English courts would uphold that choice, other than in very limited circumstances. Where there is an off-ledger ISDA Master Agreement between the parties specifying the governing law applicable to that agreement, the use of a DLT system should have no impact on this analysis.

This is regulated by Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (the "**Rome I Regulation**") as it forms part of English law by virtue of the European Union (Withdrawal) Act 2018 (as amended, the "**EUWA**"). Parties to a contract are, in principle, free to choose the law that will govern a contract between them, and Article 3 of the Rome I Regulation[3] provides that

3 Regulation (EC) 593/2008 of 17 June 2008 on the law of contractual obligations (Rome I), [2008] OJ L 177/6.

"*a contract shall be governed by the law chosen by the parties*." There are some limited exceptions to this principle (including a requirement to give effect to overriding mandatory provisions of the law of the country where contractual obligations have to be or have been performed, if those provisions render the performance of the contract unlawful),[4] but, in most cases, these exceptions are unlikely to be relevant in relation to derivatives transactions entered into under an ISDA Master Agreement in the normal course of business.

Whether an election of English law (or New York, French or Irish law) will be recognised and upheld by the courts of a third-country jurisdiction[5] will be a question of the laws of that jurisdiction.[6]

With respect to a dispute between a party to the derivative transaction and an entity responsible for the provision of the DLT system (or an aspect thereof), if the participants in the system and such entity have entered into a contractual arrangement (such as a licensing agreement and/or rulebook related to use of the DLT system) expressed to govern the contractual relationship between participants and such other entity, and containing an express choice of governing law, then that election is likely to be upheld by the English courts in accordance with the analysis set out above. The analysis will be more complicated and dependent upon the jurisdictions involved in the event that there is no such contractual arrangement in place. Such analysis is outside the scope of this chapter.

2.3.2 Jurisdiction

In the event of a dispute between the parties to a derivative transaction, where the English courts are expressed to have jurisdiction in accordance with the terms of an ISDA Master Agreement entered into between the relevant parties, the English courts will generally uphold this choice.

If the 2005 Hague Convention on Choice of Court Agreements is applicable (for example, where the parties have entered into an ISDA Master Agreement on or after 1 January 2021 and have elected in that agreement for the courts of a contracting state[7] to have exclusive jurisdiction in respect of disputes under

4 *Id.*, art. 9(3) (as it forms part of UK domestic law by virtue of the EUWA).

5 In practice, the jurisdictions most likely to be relevant would be the jurisdictions in which the parties are incorporated or from which they enter into or perform the contract.

6 We would note that the law applicable in EU member states (excluding Denmark) will be the Rome I Regulation and, as a result, the position in such member states will effectively be the same as in the UK.

7 The United States is not a contracting state, so this will not be relevant in respect of an ISDA Master Agreement providing for the courts of the State of New York to have jurisdiction. However, all EU Member States are contracting states because of the EU's accession to the

that agreement) then the English courts would be required to uphold such election and enforce any resulting judgment of the relevant court in accordance with that convention (as implemented in the UK). On the same basis, the courts of another contracting state would be required to uphold an exclusive jurisdiction clause in a contract in favour of the English courts entered into on or after 1 January 2021 (as well as to enforce any resulting judgment of the English courts).

If that Convention is not applicable, then under the common law,[8] in order for an English court to stay proceedings on the basis of England being an inappropriate forum (*forum non conveniens*), the defendant must successfully demonstrate that a foreign court is clearly more appropriate than England to try the dispute and that it is not unjust that the claimant is deprived of the right to a trial in England.[9] The mere use of a DLT system as described in the use cases identified above (even where such system has no connection to England and Wales) is highly unlikely in itself (absent other factors) to result in an English court concluding that a foreign court is more appropriate than the English courts to hear any dispute between the parties. If the parties to a contract (such as an ISDA Master Agreement) have agreed in that contract for the courts of another country (such as the courts of the State of New York) to have jurisdiction in respect of disputes between them, the English courts will respect this election and stay any claim brought in the English courts in breach of this agreement, unless the claimant can demonstrate that there are strong reasons for proceedings to continue in England.[10]

For a dispute between a party to a derivative transaction and an entity responsible in some respect for the provision of the DLT system, as with the determination of the applicable governing law, if the participants in the system and such entity have entered into a contractual arrangement which is expressed to govern the contractual relationship between participants and such other entity, and such contractual arrangement contains an express

---

Convention, so this will be relevant if the parties have entered into a French or Irish law ISDA Master Agreement (which provides, as applicable, for the relevant French and Irish courts to have exclusive jurisdiction) after the Convention became effective in the UK.

8 Following the United Kingdom's exit from the European Union and the end of the transition period, the Brussels I Regulation (recast) (Regulation (EU) No 1215/2012) ceased to apply in the United Kingdom (subject to certain transitional arrangements which are not considered here). The 2007 Lugano Convention on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters also ceased to apply.

9 *Spiliada Maritime Corp v. Cansulex Ltd* (*The Spiliada*) [1986] 3 WLR 972, [1987] AC 460 (HL) 475–478.

10 *Donohue v. Armco Inc* [2001] UKHL 64, [2002] 1 Lloyd's Rep 425.

choice of courts to hear disputes, then that election is likely to be upheld by the English courts in accordance with the analysis set out above. In the event that no such contractual arrangement is in place, the analysis will be more complex and dependent upon the jurisdictions involved. Again, such analysis is outside the scope of this chapter.

2.4 *Use of DLT with a Collateralised Transaction*

If parties wish to enter into a derivatives transaction on a collateralised basis, then, in addition to entering into an ISDA Master Agreement and a confirmation to document the terms of that transaction, they will also enter into a security or collateral agreement. This collateral arrangement is likely to be documented using one of the standard form collateral documents published by ISDA.

ISDA has published a variety of collateral documents governed by English, New York and other laws. ISDA has also published variations for use where the collateral arrangement is intended to comply with the regulatory margin requirements of one or more regimes (such as the UK regime).[11]

For the purposes of this chapter, we have not considered regulatory margin requirements[12] and have instead assumed that the parties have entered into one of the standard, non-regulatory compliant collateral documents. Excluding the collateral documentation published by ISDA in relation to compliance with regulatory margin requirements, the most frequently used English law collateral document published by ISDA is the 1995 form of ISDA Credit Support Annex, which is a title transfer[13] collateral document. The most frequently used New York law collateral document published by ISDA is the 1994 form of ISDA Credit Support Annex, which, unlike the English law version, provides for a security interest to be created over the transferred collateral. There is also an English law collateral document published by ISDA which provides for a security interest, the 1995 form of ISDA Credit Support Deed, but this is much less frequently used in the market.

---

11 The UK uncleared margin rules regime is governed by Regulation (EU) 648/2012 of 4 July 2012 on OTC derivatives, central counterparties and trade repositories ("EU EMIR") as it forms part of UK domestic law by virtue of the EUWA.

12 See ISDA, "Legal Guidelines for Smart Derivatives Contracts: Collateral" (*ISDA*, 12 September 2019) <https://www.isda.org/2019/09/12/legal-guidelines-for-smart-derivatives-contracts-collateral/> accessed 28 June 2023 for some considerations in respect to the consequences of the use of DLT where regulatory margin requirements are applicable.

13 In a title transfer collateral arrangement under English law, the collateral provider transfers full legal and beneficial ownership of the collateral to the collateral taker.

There are a number of ways in which a DLT system could be used to enhance the collateral arrangements entered into between the parties to a collateralised ISDA Master Agreement. In each case, it is not expected in the short term that parties will enter into collateralised derivatives transactions using DLT systems without also entering into an off-ledger collateral agreement documenting the terms of that collateral arrangement, such as an English law or New York law ISDA Credit Support Annex.

Similar to an uncollateralised derivatives transaction, the simplest way in which a DLT system could be used in connection with a collateralised ISDA Master Agreement would be to serve a record-keeping function, including recording the transfers of collateral that have been made between the parties. However, the actual transfers of collateral would be instructed by the parties and made outside of the DLT system, in accordance with the terms of the collateral agreement between them.

A more complex use of a DLT system would be to use it to automate certain aspects of the collateral management process. For example, the potential automation of the collateral management process in connection with collateralised derivatives transactions was considered in detail by ISDA in a 2019 paper entitled "*ISDA Legal Guidelines for Smart Derivatives Contracts: Collateral*." In that paper, ISDA identified a number of aspects of the collateral management process that could be suitable for automation, including: (i) the automation of the valuation process in respect of the determination of the amount of collateral to be transferred, and the valuation of any collateral that has previously been transferred; and (ii) the assessment of whether different types of collateral are eligible, in accordance with the eligibility criteria originally set out in the collateral document entered into by the parties.

The most complex potential use of a DLT system would be for the parties to agree that the collateral that they will exchange will be in the form of tokens that are housed on the DLT system. This could take several forms.

The first approach would be for the token to represent a real-world asset that is held and transferred off-ledger. The relevant real-world asset could continue to be transferred between the parties, as would be the case if the token did not exist. In this case, the token would serve little more than a record-keeping function and there would be very limited benefit to the use of a token in this way, in particular in relation to a security arrangement where the parties would still need to comply with any formalities in relation to taking security over the real-world asset, such as security registration requirements.

A more likely approach where the token is intended to represent a real-world asset is for the real-world asset to be immobilised (likely through being

held by a "custodian") such that when collateral is required to be transferred between the parties, there is no transfer of the real-world asset itself (which continues to be held by the custodian). Instead, the token is transferred, which results in the custodian ceasing to hold the real-world asset for the collateral provider and instead holding that asset for the collateral taker. Variations of this approach include the tokens representing a fractional interest in the real-world asset(s) or real-world assets acting as collateral for the token rather than the token being intended to represent the real world assets themselves.

A token could also be developed that purports to represent title to a real-world asset and to result in a transfer of that real world asset if the token is transferred. This is a more ambitious approach and is likely to face significant challenges. In particular, the token could become de-linked from the underlying real-world asset as a result of the real world asset being sold to a third party purchaser who is unaware of the existence of the token.

An alternative approach would be where the tokens do not represent any real-world assets but are instead assets that are "native" to the DLT system, *i.e.* solely digital tokens that may be considered to have their own intrinsic value (similar to bitcoin, which is not backed by real world assets). The parties' collateral obligations would be satisfied by the transfer of the required amount of tokens (by reference to their value) from one party to the other. This approach is likely to result in the most complex legal considerations.

2.4.1 Tokens as Property

Where the collateral that is to be transferred between parties is intended to consist of a token, the transfer of which does not result in the transfer of a real world asset (either because the real world asset that the token is linked to is immobilised and legal title to the real world asset is not transferred, or because it is a token that is native to the DLT system), an additional threshold question regarding any such arrangement is whether such token would be recognised as being property by the relevant courts.

Whether and how crypto assets (such as tokens) constitute property under English law remains the subject of ongoing legal debate. Previously, it has been argued that crypto assets do not constitute property, primarily based on the observation of Fry LJ in *Colonial Bank v. Whinney* that "all personal things are either in possession or in action. The law knows no tertium quid between the two."[14]

14 *Colonial Bank v. Whinney* [1885] 30 Ch D 261, 285.

In November 2019, the UK Jurisdiction Taskforce ("**UKJT**") published its "*Legal Statement on the Status of Cryptoassets and Smart Contracts*" (the "Legal Statement"), where it noted that this is a fundamental question, as:

> in principle proprietary rights are recognised against the whole world, whereas other – personal - rights are recognised only against someone who has assumed a relevant legal duty. Proprietary rights are of particular importance in an insolvency, where they generally have priority over claims by creditors, and when someone seeks to recover something that has been lost, stolen or unlawfully taken. They are also relevant to the questions of whether there can be a security interest in a cryptoasset and whether a cryptoasset can be held on trust.

The UKJT concluded that a crypto asset, such as a token, will not constitute a *chose* in possession as it is not tangible and therefore is not capable of possession. It could be argued that, in accordance with the dicta of Fry LJ, it is necessary for a crypto asset to constitute a *chose* in action in order to constitute property. The UK Jurisdiction Taskforce were not convinced by this argument and noted in the Legal Statement: "[o]ur view is that Colonial Bank is not therefore to be treated as limiting the scope of what kinds of things can be property in law. If anything, it shows the ability of the common law to stretch traditional definitions and concepts to adapt to new business practices."[15] The Legal Statement went on to conclude that "the fact that a cryptoasset might not be a thing in action on the narrower definition of that term does not in itself mean that it cannot be treated as property"[16] and that crypto assets should be treated "in principle as property."[17]

In December 2020, the High Court in *Ion Science Ltd v. Persons Unknown and others*[18] accepted the analysis in the UKJT's Legal Statement, concluding that a crypto asset such as bitcoin was a form of property capable of being the subject of a proprietary injunction. This decision is one of a series of interim rulings from the English courts which suggest that crypto assets can be treated

15 UK Jurisdiction Taskforce, "Legal statement on cryptoassets and smart contracts" (*The Law-Tech Delivery Panel*, November 2019), 20 <https://35z8e83m1ih83drye28009d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf>" with "<https://www.blockchain4europe.eu/wp-content/uploads/2021/05/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf>.

16 *Id*., para 84.

17 *Id*., para 85.

18 *Ion Science Ltd v. Persons Unknown and others* (unreported), (Comm, 21 December 2020).

as property within the common law definition of the term, and which have relied at least in part on the UKJT's Legal Statement.[19]

The premise that crypto assets such as tokens should in principle be treated as property has been broadly accepted by legal practitioners and we would expect this position to continue to be upheld by the English courts. Nonetheless, there is still uncertainty in respect of some points of law, including exactly how crypto assets constitute property and, for example, whether a third category beyond *choses* in possession and *choses* in action could be said to exist.

Following the publication of the UKJT's Legal Statement, the UK Government asked the Law Commission to analyse the current law applicable to smart contracts and digital assets, and to identify appropriate options for reform to accommodate these technologies. The Law Commission responded by issuing, on 30 April 2021, a call for evidence on the legal position of digital assets.[20] The Law Commission hopes to clarify how digital assets are being used and particularly addresses the question of whether crypto assets should be "possessable" under English law. The call for evidence was followed by the publication of an interim update paper on 24 November 2021.[21] That update paper noted that many respondents to the call for evidence had proposed that it may be helpful for digital assets to be categorised as belonging to a new third category of personal property which is distinct from things in action and things in possession. The interim update paper is expected to be followed by a consultation paper in mid-2022 which will consider this in greater detail.

Having further certainty around how crypto assets (such as tokens) constitute property (and the implications that this has, including in relation to custody, insolvency, and security interests applicable to digital assets) will greatly assist market participants and result in more extensive use of digital assets across financial services, including in a derivatives context.

2.4.2 Admissibility in Evidence

An additional complication that could in theory arise from the use of tokens in connection with a collateralised derivative transaction (or more generally in connection with the use of a smart contract) is whether a token (or smart

19 See also the High Court's decision in *AA v Persons Unknown* [2019] EWHC 3556 (Comm), [2020] 4 WLR 35, which recognised unlawfully obtained bitcoin as property which is capable of being subject to a proprietary injunction.

20 Law Commission, "Digital assets Call for evidence" (*Law Commission*, 30 April 2021) <https://www.lawcom.gov.uk/project/digital-assets/> accessed 28 June 2023.

21 Law Commission, "Digital assets Interim Update" (*Law Commission*, 24 November 2021) <https://www.lawcom.gov.uk/project/digital-assets/> accessed 28 June 2023.

contract) in electronic form would be admissible in evidence in the relevant courts.

Where the relevant courts are the English courts, this should not be an issue. The admissibility of electronic documents in court proceedings is governed by the Electronic Communications Act 2000. Pursuant to that Act, an electronic document is admissible in evidence in relation to any question over the authenticity of an electronic transaction.[22]

Electronic Documents are defined broadly as "anything stored in electronic form, including text or sound, and visual or audiovisual recording."[23] As a result, the term Electronic Document has a far broader meaning than the use of the term 'document' may suggest and should in theory encompass a token (or smart contract), provided that transactions in respect of such token are capable of being reproduced in a format that can be read by the court.

However, the Law Commission's call for evidence on the legal position of smart contracts highlighted some possible concerns.[24] For example, it is possible that the way in which smart contracts are programmed, *i.e.* whether in source code, which is (to some extent) human-readable, or binary form, which is not generally legible by humans, could lead to discrepancies in terms of whether they constitute "writing" under English law, which in some cases may impact admissibility. This is one of many issues under consideration by the Law Commission, which, following its analysis of the current law applicable to smart contracts, aims to identify appropriate options for reform.

2.4.3 Determining the Law Applicable to the Transfer of Collateral

The use of a DLT system could potentially complicate the analysis regarding the law(s) that will be applicable for the transfer of collateral from a collateral provider to a collateral taker, whether pursuant to a title transfer collateral arrangement (such as under an English law Credit Support Annex), or pursuant to a security arrangement (such as under a New York law Credit Support Annex).

Where, notwithstanding the use of a DLT system, there is a transfer of a real-world asset from the collateral provider to the collateral taker (*i.e.* where the DLT system, or the transfer of a token under a DLT system, serves only a

22 UK Electronic Communications Act 2000, sec. 7C(2). The term "electronic transaction" is not defined.

23 *Id.*

24 Law Commission, "Smart contracts" (*Law Commission*, 25 November 2021) <https://www.lawcom.gov.uk/project/smart-contracts/> accessed 28 June 2023. The consultation closed in March 2021, and following the consultation, the Law Commission published Advice to the Government in November 2021.

record-keeping function), then, in practice, the use of the DLT system should not change the analysis that would apply where no DLT system is being used.

Where there is no transfer of a real world asset but there is a transfer of a token under a DLT platform (either because the token is linked to a real world asset but that real world asset is immobilised and will not itself be transferred between collateral provider and collateral taker, or because it is a token native to the DLT system which is itself being used to satisfy the relevant collateral call) the law applicable to the transfer of collateral will need to be determined by reference to the token itself.

The existing laws relating to proprietary interests in assets may not be easy to apply to tokens as they have been developed by reference to other types of assets. The collateral currently predominantly used in connection with derivatives transactions is securities. At a high level, a token on a DLT system may seem similar to a security held in book-entry form with a central securities depository. However, there are significant differences which mean that it is not simply the case that the laws applicable to the transfer of securities held in a central securities depository can be applied equally to a token held in a DLT system.

Under English law, in relation to a transfer of securities pursuant to a collateral arrangement (whether by means of a title transfer collateral arrangement or a security arrangement), the Financial Markets and Insolvency (Settlement Finality) Regulations 1999 (as amended) as they form part of English domestic law by virtue of the EUWA provide that where a security is provided as collateral and "a register, account or centralised deposit system legally records the entitlement of" the relevant person to that security, then "the rights of that person as a holder of collateral security in relation to those securities are governed by the domestic law of the country or territory or, where appropriate, the law of the part of the country or territory, where the register, account, or centralised deposit system is maintained."[25] This is effectively an application of what is known as the Place of the Relevant Intermediary Approach ("**PRIMA**") principle, pursuant to which to determine the law applicable to the proprietary aspects of a transaction in securities (such as a collateral transfer) it is not necessary to look through the various chains of intermediaries holding indirect interests in the underlying securities but, instead, it is necessary only to consider the laws applicable in respect of the intermediary immediately above the parties.

25 UK The Financial Markets and Insolvency (Settlement Finality) Regulations 1999, Regulation 23.

In contrast, where the parties are transferring a token held on a DLT system, there will be no centralised depository holding the token (nor is the token necessarily held in an account with an intermediary). Instead, the token is recorded on the distributed ledger and each participant in the DLT system has an equal record of the transactions in respect of that token. As a result, the ledger (and the token) could effectively be located in multiple jurisdictions (depending upon the location of the participants in the DLT system).

In recent years, financial transactions referencing tokens, including transactions secured over such tokens (in particular bitcoin and ether), have become more common. With respect to such secured transactions, parties have had to address how to take effective security over the token notwithstanding the uncertainties identified above. The approach taken is often to dispossess the security provider from the relevant token. This may be pursuant to the use of a pledge in a civil law jurisdiction (although this approach would not be used under English law) or by providing for the token to be held by a "custodian"[26] with (in addition to any security granted over the token itself) security taken over the rights that the security provider has vis-à-vis the custodian under the relevant custody agreement. Whilst the use of a custodian in this way may, at first sight, appear similar to the use of custodians when taking security over securities held in custody, in practice there will be important differences. For example, as noted above, the PRIMA principle would not apply under English law where the custodian holds tokens rather than securities. In addition, depending upon the jurisdiction of the custodian, the rules relating to custodians holding client assets (and their segregation from the estate of the custodian upon its insolvency) may not apply.

3 Possible Options for Determining the Law Applicable to the Transfer of a Token

In a paper entitled "*Distributed Ledger Technology and Governing Law: Issues of Legal Uncertainty*," published in March 2018 (the "**FMLC Paper**"),[27] the Financial Markets Law Committee considered the conflict-of-laws issues that may

26 We use the term custodian here, although other terminology is also frequently used for this role with respect to digital assets.

27 Financial Markets Law Committee, "Distributed Ledger Technology and Governing Law: Issues of Legal Uncertainty" (*Financial Markets Law Committee*, March 2018) <http://fmlc.org/report-finance-and-technology-27-march-2018/> 28 June 2023.

arise from the use of DLT systems[28] and recommended that "As the law relating to DLT lags behind the trajectory of the technology, an international conflict of laws framework for financial transactions and systems using DLT needs to be developed as a matter of priority."[29] The FMLC Paper identified a number of possible options that legislators could adopt in respect of choice of law rules for the proprietary effects of transactions conducted on DLT systems, including in relation to tokens where there is no related transfer of a real world asset.

One option considered was what the FMLC Paper refers to as an "elective *situs*" approach. Pursuant to this approach, the law applicable to the proprietary effects of transactions (such as derivatives transactions) entered into on a DLT system would be the law of the jurisdiction chosen by the participants in the DLT system.

The FMLC Paper noted that the advantages of this approach include that the applicable governing law would be the same for all transactions entered into on the relevant DLT system, and therefore the applicable governing law would be transparent to all parties involved.

However, the FMLC Paper also identified certain potential disadvantages in respect of this approach, including, in particular, that allowing participants in the DLT system such freedom of choice would enable them to pick any governing law, even a law which has no connection to the tokens and parties involved, which may not be seen as desirable by regulators. To address this concern, the FMLC Paper proposed as an alternative a "modified elective *situs*" approach, pursuant to which the participants' right to choose the applicable governing law is "limited to a choice of law approved by regulators, or restricted in respect of a choice of law lacking any connection to the DLT enterprise."[30]

The FMLC Paper identified a number of other possible approaches to identifying the law that should be applicable to the proprietary effects of transactions conducted on DLT systems but concluded that "elective *situs* should be the starting point for any analysis of a conflicts of law approach to virtual tokens. This solution meets the requirements of being objective and easily ascertainable by the parties themselves, and provides the clearest route for establishing the governing law within the context of this new technology."

These issues were also considered specifically in the context of derivatives in a paper published by ISDA, Clifford Chance, R3 and the Singapore Academy of Law in January 2020 entitled "*Private International Law Aspects of Smart*

28 The paper considered the use of DLT systems generally in relation to transactions in financial instruments or assets rather than derivatives transactions specifically.

29 Financial Markets Law Committee (n 27), 5.

30 *Id.*, 16.

Derivatives Contracts Utilizing Distributed Ledger Technology."[31] That paper also recommended the use of the elective *situs* approach:

> [i]t would therefore provide greater clarity for all parties to agree that their transactions should be subject to a common 'law of the platform', 'law of the system', or elective situs – that is, a uniform choice of law that the parties agree will govern all on-ledger transactions. Such common law of the platform could then be used as the situs of any tokens that are native to that DLT system. Where national authorities and regulators are concerned that allowing parties an unfettered choice of a governing law of the platform is undesirable, the choice of law could be restricted to the laws of countries where parties such as the issuer of assets, the system administrator and market participants are subject to sufficient legal and regulatory oversight.

A form of elective situs would be a logical approach to adopt in the context of DLT systems, in particular private DLT systems where the participants in the DLT system can all be known to each other and can expressly agree to the governing law that should apply to the aspects of their transactional relationship that would not be covered by an off-ledger agreement (such as an ISDA Master Agreement). This would include the law applicable to the proprietary aspects of a transaction in respect of a token that is native to the DLT system.

Given the increasing use of custodians in relation to secured transactions over crypto assets (such as bitcoin and ether), distinct rules could also be developed in relation to tokens held in custody. This could be based on a modified version of the PRIMA principle (based on the location of the custodian or wallet).

Whilst individual jurisdictions (or individual states within the United States) may look to legislate on such issues, this may in due course lead to a fragmentation of approaches and the potential for conflict-of-laws issues regarding transactions using DLT systems. As a result, it would be preferable to have cross-jurisdictional cohesion, either through a broadly harmonised approach being adopted by different national governments or, more practically, established at the instigation of one of the international standard-setting

31 ISDA et al., "Private International Law Aspects of Smart Derivatives Contracts Utilizing Distributed Ledger Technology" (*ISDA*, January 2020) <https://www.isda.org/a/4RJTE/Private-International-Law-Aspects-of-Smart-Derivatives-Contracts-Utilizing-DLT.pdf> accessed 28 June 2023 (The present author contributed to that paper, and it has partially influenced the analysis in this chapter.).

bodies (such as the Hague Conference on Private International Law, UNIDROIT or UNCITRAL).

There is significant interest in the use of DLT systems for financial markets transactions (including with respect to the derivatives markets) and the use of DLT systems for such purposes is likely to significantly increase over the next decade. The development of a cross-border framework regarding the use of DLT systems (including in terms of the proprietary aspects of transactions in tokens on DLT systems) would provide significant comfort to market participants when it comes to adopting such new technologies, and would likely assist with the development of the market in financial transactions using DLT.

PART 4

Blockchain & Dispute Resolution

CHAPTER 20

Blockchain Dispute Resolution for Decentralized Autonomous Organizations: The Rise of Decentralized Autonomous Justice

Florence Guillaume and Sven Riva

1 Introduction

For the past twenty years, the use of the Internet has facilitated international commercial relations between people who do not know each other and who are geographically distant. International civil litigation has increased exponentially with the development of e-commerce. Disputes associated with e-commerce have undermined the supremacy of state courts, which have proved unable to provide an appropriate response to small claim disputes arising in an international context. The length, cost and complexity of the procedure stemming from delicate questions as to jurisdiction and applicable law, as well as the risk associated with the international enforcement of the decision are deterrent factors that led e-commerce platforms to develop Online Dispute Resolution (ODR) mechanisms (ODRS).

Thanks in part to the removal of intermediaries, the transfer of cryptocurrencies and other crypto assets using blockchain technology has further facilitated international commercial relations. The emergence of smart contracts has revolutionised the way people enter into contractual relationships by dematerialising the parties' agreement. The decentralised and distributed characteristics of blockchain technology and the pseudonymity of crypto transactions has led to a new economy growing independently from nation states, the so-called "crypto economy". The use of this technology has brought an additional degree of complication in the application of Private International Law (PIL) rules by removing the illusion that online transactions can always be linked, in some way or another, to the territory of a state. Online transactions operated via a public blockchain are inherently transnational and require the application of connecting factors that are not always adapted.[1] Smart contracts

1 Florence Guillaume, "Blockchain: le pont du droit international privé entre l'espace numérique et l'espace physique," in Ilaria Pretelli (ed), *Conflict of Laws in the Maze of Digital Platforms* (Schulthess 2018), 163, 175.

© FLORENCE GUILLAUME AND SVEN RIVA, 2023 | DOI:10.1163/9789004514850_022
This is an open access chapter distributed under the terms of the CC BY-NC-ND 4.0 license.

even allow the creation of digital entities that are governed in an autonomous and decentralised manner by computer code. Those entities are central players in the crypto economy and are used to enter into commercial relations in the emerging Decentralized Finance (DeFi) ecosystem. The first Decentralized Autonomous Organization (DAO) was the source of a resounding dispute between parties with diverging interests, which had to be urgently resolved without any access to state justice or a dispute resolution mechanism. This case revealed the risk of disputes in the blockchain environment as well as the legal uncertainty related to crypto transactions, which led to the emergence of blockchain-based Dispute Resolution (BDR) mechanisms (BDRs) inspired by the private justice systems developed in e-commerce.

This chapter examines the resolution of disputes involving DAOs. The authors first analyse the concept of DAOs and their role in the crypto economy. The focus is on whether DAOs qualify as companies in the legal sense. What is at stake is the legal personality of DAOs and their capacity to conduct legal proceedings in state courts (2). The authors then consider how to determine jurisdiction for disputes involving DAOs. Two types of disputes will be discussed: disputes related to the governance of a DAO, and disputes arising from a contractual relationship between a DAO and a third party. This will highlight the difficulties in determining jurisdiction of state courts related to the impossibility to locate and the pseudonymity of actors of the crypto economy (3). The practical problems of resolving those kinds of disputes before a state court will lead the authors to consider the use of ODRs. Those dispute resolution mechanisms have proven their worth for online transactions, particularly in the field of e-commerce (4). It is not surprising that ODRs are inspiring the development of new dispute resolution mechanisms that integrate blockchain technology and are designed to take into account the particularities of the crypto environment (5). The main characteristics of existing BDR models which are adapted to the resolution of disputes involving DAOs will be described in order to show whether and how BDRs are likely to avoid a denial of justice by granting access to justice to DAOs (6). The authors then examine the fairness of BDR decisions in order to determine whether this type of decision is likely to provide effective access to justice for DAOs. The authors will then address the delicate issue of the scope of BDR decisions in state jurisdictions and their off-chain enforcement (7), before concluding with a few words on the legitimacy of BDRs (8).

2 Decentralized Autonomous Organization (DAO)

DAOs are new forms of entities that are being used to organise economic and social activities in the blockchain environment. As the concept of a DAO is still

relatively unknown, a clear definition must be established before addressing the need for conflict resolution mechanisms adapted to those entities (2.1). The vast majority of DAOs are created outside the law, which exposes their members as well as the persons contracting with them to a high degree of legal uncertainty (2.2). Existing PIL rules can be used to clarify the legal scope of DAOs and provide legal certainty and predictability to a growing global ecosystem of financial services (2.3).[2]

2.1 *Notion of DAO*

Since the early days of Bitcoin, blockchain enthusiasts envisioned a new form of digital company for which management rules would be distributed across all the nodes of a blockchain network in order to be incorruptible. Cryptocurrencies would constitute the shares of this digital company and, as cryptocurrencies have market value, they would also serve as the assets of the company.[3] This is how the idea of the "virtual corporation"[4] came to light: a new form of company that would rely on the security, predictability and speed of computer code and would remove the need for human involvement as much as possible to minimise error and corruption within the company's affairs. The ultimate stage of the virtual corporation will be met when artificial intelligence will allow the company to run itself entirely autonomously.

However, the Bitcoin protocol did not allow for such complex rules to be coded, which pushed – *inter alia* – for the development of a new type of blockchain. Well-known blockchain entrepreneur Vitalik Buterin co-developed in 2013 the Ethereum blockchain, which allowed cryptocurrency transactions to be subject to a set of rules through a mechanism called "smart contract."[5] This term was originally used by computer scientist and legal scholar Nick Szabo who, in 1994, defined a smart contract as "a computerized transaction protocol that executes the term of a contract."[6] Smart contracts programmed on the Ethereum blockchain allow the transfer of cryptocurrencies to be automated and conditioned to a set of programmed rules. The smart contract can also be

2 This chapter includes analysis elements that have already been developed in Sven Riva, "Decentralized Autonomous Organizations (DAOs) in the Swiss Legal Order" (2019/2020) 21 Yearbook of Private International Law 601.

3 For a brief description of the origins of DAOs, see Riva (n 2), 607–610.

4 Vitalik Buterin, "Bootstrapping A Decentralized Autonomous Corporation: Part 1" (*Bitcoin Magazine*, 20 September 2013) <https://bitcoinmagazine.com/technical/bootstrapping-a-decentralized-autonomous-corporation-part-i-1379644274> accessed 5 November 2021.

5 Nick Szabo, "Smart Contracts" (1994) <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html> accessed 5 November 2021.

6 Szabo (n 5).

programmed to gather information from an external source, called an "oracle," to trigger the execution of the transfer of cryptocurrencies.[7] The legal doctrine has widely analysed smart contracts to determine their legal scope.[8] This frenzy results from the term "contract" in "smart contract," which suggests that the computer code is a contract in the legal sense. However, the use of this term is misleading since a smart contract is not necessarily a contract in the legal sense. It depends both on the characteristics of a particular smart contract and the definition of a contract in the applicable law. Some states have decided to explicitly give legal effect to certain smart contracts,[9] while in other states their legal scope is still disputed.[10]

According to Buterin, DAOs are the logical extension of smart contracts as they are nothing else than "long-term smart contracts that contain the assets and encode the bylaws of an entire organization."[11] What differentiates a DAO from a smart contract is that a DAO has some form of internal organisation that defines the governance of the entity and establishes the procedure to manage

7 An example would be a smart contract programmed to execute the transfer of 10 ETH if the price of ETH reaches a predefined level. To know the price of ETH, the smart contract would rely on an oracle, which in our example could be a designated exchange.

8 For Swiss literature, see Olivier Hari and Ulysse Dupasquier, "Blockchain And Distributed Ledger Technology (DLT): Academic Overview Of The Technical And Legal Framework And Challenges For Lawyers" (2018) 5 International Business Law Journal 423, 443–444; Blaise Carron and Valentin Botteron, "Le droit des obligations face aux 'contrats intelligents'," in Blaise Carron and Christoph Müller (eds), *3e Journée des droits de la consommation et de la distribution, Blockchain et Smart Contracts – Défis juridiques* (Helbing Lichtenhahn 2018), 1; Christoph Müller, "Die Smart Contracts aus Sicht des Schweizerischen Obligationenrechts" (2019) 5 Zeitschrift des Bernischen Juristenvereins 330; Andreas Furrer, "Die Einbettung von Smart Contracts in das schweizerische Privatrecht" (2018) 3 Anwaltsrevue 103; Mirjam Eggen, "Smart Contracts und allgemeine Geschäftsbedingung," in Susan Emmenegger and others (eds), *Brücken bauen: Festschrift für Thomas Koller* (Stämpfli 2018), 155; Florian Möslein, "Smart Contracts im Zivil- und Handelsrecht" (2019) 183 Periodical for Overall Commercial and Business Law 254.

9 *E.g.*, Arizona House Bill 2417 of 29 March 2017; Section 5 of the Illinois Blockchain Technology Act House Bill 3575 of 23 August 2019; Section 34-29-103 of the Wyoming Bill SF 0125 of 1 July 2019 amending Article 9 of the Wyoming Uniform Commercial Code.

10 This is the case in Switzerland where some authors (see *e.g.*, Furrer (n 8), 106) argue that in some instances a smart contract can qualify as a contract in the legal sense, while others (see *e.g.*, Müller (n 8), 344) argue that smart contracts lack prerogatives required by law to qualify as contracts.

11 Vitalik Buterin, "Ethereum White Paper – A Next Generation Smart Contract & Decentralized Application Platform" (*Blockchain Lab,* November 2013) <https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf> accessed 5 November 2021.

its crypto assets, while smart contracts are simple rules that trigger the transfer of crypto assets when determined conditions are met.

A DAO can be defined as "the entity created by the deployment of an autonomous and self-executing software running on a distributed system that allows a network of participants to interact and manage resources on a transparent basis and in accordance with the rules defined by the software code."[12] The participants of a DAO benefit from the pseudonymity of the blockchain environment[13] and can only be identified by their public key, which is their wallet address. There is no link to their "real" identity except in circumstances where they are using regulated services that require Know Your Customer (KYC) identification. With pseudonymity, the only barrier for becoming a member of a DAO is usually economic, meaning that DAOs can potentially be joined by anyone from anywhere in the world.[14] As such, a DAO must be considered as a community of unreliable members. In order for DAOs to function, their architecture must take this key characteristic into account.

The governance rules of DAOs are inscribed on smart contracts. They benefit from the immutability of the blockchain infrastructure[15] and certain aspects of their governance are automated, "reducing operational costs and improving internal controls while simultaneously increasing the overall transparency of [the] organization."[16] When a member or a group of members wish to undertake an action through the DAO, they must submit a proposal to the community, which will either be accepted and executed, or refused. This allows unreliable members to collaborate in the pursuit of a common goal. Their participation is ensured through crypto-economic incentives that reward beneficial behaviour. Those mechanisms are inspired from the ones that allow public blockchains

12 Riva (n 2), 614.

13 See Primavera De Filippi and Aaron Wright, *Blockchain and the Law* (Harvard University Press 2018), 38–39.

14 One known exception is NEDAO, which is a DAO being developed as a community project for the people of the canton of Neuchâtel, Switzerland. To join NEDAO, members must have their public key certified with the residents' office to prove that they reside in the canton of Neuchâtel. However, their pseudonymity is safeguarded as their public key is not linked to their identity. See <https://nedao.ch> accessed 5 November 2021.

15 See Kevin Werbach, "The Siren Song: Algorithmic Governance by Blockchain," in Kevin Werbach (ed), *After the Digital Tornado – Networks, Algorithms, Humanity* (Cambridge University Press 2020), 215.

16 The LAO, "The LAO: A For-Profit, Limited Liability Autonomous Organization" (*Medium*, 3 September 2019) <https://medium.com/openlawofficial/the-lao-a-for-profit-limited-liability-autonomous-organization-9eae89c9669c> accessed 5 November 2021.

such as Bitcoin and Ethereum to function as global networks.[17] Furthermore, the smart contracts which contain a DAO's governance rules are spread on all the computers of the blockchain network. No person, entity or government has the power to update or alter the code in a contrary manner to what is provided for in the governance rules. Consequently, DAOs that exist on a public blockchain such as Ethereum are assumed to be transnational, autonomous, and censorship resistant.[18]

The first widely known DAO was a form of venture capital fund called "The DAO" which was launched in 2016 on the Ethereum blockchain. Participants could submit projects to be funded and the decision-making process was distributed between the approximatively 10000 token holders of The DAO. With the equivalent of then USD 150 million invested in The DAO within a few weeks, this was the largest crowdfunding project of its time. The founders of The DAO attempted "to set up a corporate-type organization without using a conventional corporate structure."[19] Agency relationships between investors and other actors found in a traditional firm were replaced by encoded governance rules. The code also provided minority shareholder protections by allowing small investors to exit The DAO and retrieve their investment under certain conditions. Unfortunately, a hacker found a bug in the minority shareholder protection mechanism and was able to drain The DAO from a large portion of its funds. This put an immediate stop to the project and outlined the risks associated with blockchain technology. As no state authority had jurisdiction over The DAO or the Ethereum blockchain, participants had no recourse to retrieve their investment. However, as a huge portion of existing ethers were invested in The DAO and the hack put the whole blockchain in jeopardy, key players pushed for the transactions triggered by the hacker to be reversed to protect the interests of the Ethereum community. A version of the Ethereum blockchain that did not contain the hacker's transactions was released, resulting in a hard fork of the blockchain. This meant departing from the "code is law" doctrine[20] that drives the blockchain environment. Tempering with the

17 Bitcoin and Ethereum can be considered DAOs. Riva qualified those blockchains as "ground layer DAOs," as opposed to "top layer DAOs" running on their infrastructure. See Riva (n 2), 616.

18 Riva (n 2), 620. See also Guillaume (n 1) who states that using a public blockchain is enough to confer an international scope upon a transaction.

19 Wulf A. Kaal, "Blockchain-Based Corporate Governance" (2021) 4 Stanford Journal of Blockchain Law & Policy 0, 6.

20 This doctrine was developed by Lawrence Lessig in his article "Code Is Law – On Liberty in Cyberspace" (*Harvard Magazine*, 1 January 2000) <https://harvardmagazine.com/2000/01/code-is-law-html> accessed 5 November 2021. He established the principle

state of the ledger prompted a lot of debate at the time and could probably not happen again. Even though The DAO project was not a success *per se*, it was a learning experiment for the blockchain community. It became evident that if the Ethereum blockchain is to be a trusted infrastructure, immutability is key, and the ledger should never again be tampered with. This case showed that if the blockchain ecosystem was to thrive as an economic powerhouse, the system had to provide adapted dispute resolution mechanisms to smart contract and DAO users.

Today, online platforms such as Aragon[21] and DAOstack[22] offer templates of DAOs that are preconfigured to undertake different types of projects such as a charity, a freelance network, or a venture fund. DAOs offer alternatives to existing corporate structures by enabling pseudonymous actors from all around the world to define and adhere to their own decentralised organisational structures to pursue economic and social activities.[23] Being much more adapted for financial business in the blockchain environment than traditional legal vehicles offered by states, DAOs have been extensively used in the fast-growing DeFi ecosystem once valued at USD 100 billion.[24] With that much capital, DeFi "expands the use of blockchain from simple value transfer to more complex financial use cases."[25] As such, new ways to organise economic coordination are emerging from the blockchain environment. But DAOs also allow for other types of economic and social entities to exist in the blockchain environment. For example, Kleros and Aragon Court are, to this day, DAOs that offer dispute resolution mechanisms to actors of the crypto economy, thus providing the blockchain environment with its own private justice.[26]

---

that code regulates behaviour on the Internet. This idea is very popular in the blockchain ecosystem, where it is generally accepted that the only rules that can regulate behaviour within a system (such as a blockchain) are the ones set in the code. Any participant to a blockchain system agrees to the rules of the code and any behaviour allowed by the code is right.

21 <https://aragon.org> accessed 5 November 2021.

22 <https://daostack.io> accessed 5 November 2021.

23 See Kaal (n 19), 2–3; Jonathan Rohr and Aaron Wright, "Blockchains, Private Ordering, and the Future of Governance," in Philipp Hacker and others (eds), *Regulating Blockchain – Techno-Social and Legal Challenges* (Oxford University Press 2019), 43, 47–50.

24 Brady Dale, "DeFi Is Now a $100B Sector" (*Coindesk*, 29 April 2021) <https://www.coindesk.com/defi-100-billion-sector> accessed 5 November 2021.

25 Alyssa Hertig, "What is DeFi?" (*Coindesk*, 18 September 2020) <https://www.coindesk.com/what-is-defi> accessed 5 November 2021.

26 See *infra* chapters 5 and 6.

2.2 *Practical Implications of Recognising DAOs as Legal Entities*

The key role that DAOs play in the ever-growing crypto economy and the development of DeFi has driven some states to introduce legislation that would allow DAOs to exist within their jurisdiction. By providing a legal framework for DAOs, some states are expecting to become the go-to place for crypto enthusiasts to pursue crypto-economic activity. Those legal frameworks could help states to regulate the crypto economy while benefiting from new sources of tax revenue.

DAOs that are created and incorporated under the laws of a state will hereafter be referred to as "regulated DAOs." However, the vast majority of DAOs are still being created outside existing legal frameworks and are not incorporated within a state jurisdiction. Those DAOs will hereafter be referred to as "maverick DAOs."[27]

As DAOs are used as a means to combine resources in a common enterprise, relationships are automatically created among the members of a DAO. Regulated DAOs benefit from a legal framework that defines the nature of those relationships. For example, some legislation introduces a legal fiction, which grants DAOs a legal personality detached from their members' personality as well as limited liability for the members so that they are not at risk if the DAO fails. However, maverick DAOs cannot automatically benefit from those legal constructs of corporate law. As with limited liability, "[l]egal personality cannot be created through private agreements or actions."[28] Legal personality is a fiction of the law granted by state jurisdictions to some forms of companies that are constituted within their legal framework. Limited liability must also stem from the law and is granted to the members of some forms of companies. As most DAOs are constituted outside the law, their members do not benefit from a clear legal framework and the legal nature of their relationships is uncertain. This leaves members of maverick DAOs exposed to legal uncertainty with respect to their legal liability should there be a dispute of contractual, tortious, criminal, or administrative nature.

DAOs are destined to eventually enter into business relationships with third parties, for example by buying or selling services and crypto assets. The legal capacity of regulated DAOs is defined by the law, which ensures their activities have a legal scope. However, just as the legal nature of maverick DAOs is not

27 According to the terminology adopted by Riva (n 2).

28 Max Ganado, Joshua Ellul, Gordon Pace, Steven Tendon and Bryan Wilson, "Mapping the Future of Legal Personality" (*MIT Computational Law Report*, 20 November 2020), 10 <https://law.mit.edu/pub/mappingthefutureoflegalpersonality/release/1> accessed 5 November 2021.

certain, so is their legal existence. This begs the question of whether maverick DAOs can be parties to a contract. For a DAO to be able to validly enter into a contractual relationship, it must have legal capacity. If a DAO enters a legally binding commitment without having legal capacity, individual members of the DAO could find themselves personally bound by the resulting legal obligations. If individual members of the DAO could not be identified – because of their pseudonymity –, the contract could end up being qualified as legally void. As long as the contract is well executed, those questions can be set aside. However, they are of particular importance when a dispute arises between a DAO and its contracting party.

2.3 *Legal Status of DAOs*

To analyse the legal status of DAOs, we will first proceed with maverick DAOs and consider the lack of legal framework for those entities. We will determine the nature of the legal relationships that are created among the members of a maverick DAO, between the members and the DAO itself, and the possibility for these DAOs to enter into legal relationships with third parties (2.3.1). Then, we will examine the legislation of three states that allow DAOs to exist within a legal framework. For each of the categories of regulated DAOs, we will first address their legal nature to identify the legal regime to which they are subject. This will allow us to determine their legal capacity and the legal scope of the relationships among the members, between the members and the DAO, and with third parties (2.3.2).

2.3.1 Maverick DAOs

Trying to determine the legal nature of maverick DAOs is a legally challenging undertaking and the resulting answer could differ from one maverick DAO to another, and from one jurisdiction to another. Since DAOs function as organisational structures pursuing economic or social activities, the core question is whether a certain maverick DAO can be considered a company (or another form of organisation), in which case the relationships among the members of the DAO would be ruled by corporate law (and laws governing other forms of organisations), or if the DAO should be regarded as a simple partnership, in which case the relationships among the members of the DAO would be of a contractual nature.[29] But the key challenge is finding which law should

29 For a full analysis of the application of simple partnership regimes of different states to DAOs, see António Garcia Rolo, "Challenges in the Legal Qualification of Decentralized Autonomous Organizations (DAOs): The Rise of the Crypto-Partnership?" (2019) 1 Revista de Direito e Tecnologia 33, 63–72.

determine whether or not a DAO should be qualified as a company and which legal rules should apply. As maverick DAOs do not stem from the laws of a particular jurisdiction, some authors have attempted to apply by analogy existing company law rules of their own jurisdiction to define the legal regime of maverick DAOs.[30]

If we complete this exercise from the point of view of Swiss law, the first step to undertake when confronted with a maverick DAO is to determine whether it qualifies as one of the forms of companies provided in the law, mainly the Code of Obligations (CO)[31] and the Civil Code (CC).[32] A company (or partnership) is defined under Article 530 para. 1 CO as "a contractual relationship in which two or more persons agree to combine their efforts or resources in order to achieve a common goal." When a partnership does not fulfill the distinctive criteria of other forms of partnerships (*i.e.*, other forms of companies), it is to be qualified as a simple partnership (Article 530 para. 2 CO). As Swiss corporate law does not provide for a "Swiss DAO," it is safe to say that, to date, no DAO meets legal requirements of any form of company as regards to its structure (requirement of certain corporate bodies) and/or its publicity (requirement to be registered in the Swiss company register).[33]

The question remains as to whether a DAO qualifies as a simple partnership (*société simple*), in which case it must be regarded as a multilateral contractual relationship and not a company.[34] As a DAO does not fall within one of the specific forms of companies under Swiss law, Swiss courts, confronted with a DAO, would probably have no choice but to qualify the organisation as a simple

30 Matthias P.A. Müller, "Blockchain und Gesellschaftsrecht: ein Streifzug durch Möglichkeiten und Hürden: unter besonderer Berücksichtigung der Decentralized Autonomous Organization" (2019) Expert Focus: Schweizerische Zeitschrift für Wirtschaftsprüfung, Steuern, Rechnungswesen und Wirtschaftsberatung 485; Martin Hess and Patrick Spielmann, "Cryptocurrencies, Blockchain, Handelsplätze & Co. – Digitalisierte Werte unter Schweizer Recht," in Thomas U. Reutter and Thomas Werlen (eds), *Kapitalmarkt – Recht und Transaktionen XII* (Schulthess 2017), 145; Alexander F. Wagner and Rolf H. Weber, "Corporate Governance auf der Blockchain" (2017) Schweizerische Zeitschrift für Wirtschafts- und Finanzmarktrecht 59, 67.

31 Federal Act of 30 March 1911 on the Amendment of the Swiss Civil Code (Part five: The Code of Obligations) (SR 220).

32 Swiss Civil Code of 10 December 1907 (SR 210).

33 Same opinion: Hess and Spielmann (n 30). See also Delphine Yerly and Charlotte Boulay, "Fintech, Bitcoins, Blockchains, Decentralized autonomous organizations (DAOs): the future is bright, the future is decentralized – Intervention by Olivier Hari: Cryptocurrencies and DAO" (*Jusletter IT Flash*, 26 January 2017), para. 15.

34 François Chaix, "Art. 530 CO," in Pierre Tercier, Marc Amstutz and Rita Trigo Trindade (eds), *Code des obligations II – Commentaire romand* (2nd edn, Helbing Lichtenhahn 2017), para. 2.

partnership. However, the pseudonymity of DAO members contradicts the personal structure of the simple partnership, which requires from the partners to be faithful and loyal to each other.[35] Furthermore, each partner of a simple partnership is jointly and severally liable for the debts contracted within the framework of the partnership. This legal regime is not fit for DAOs as it would not be conceivable to expect from the members of a maverick DAO to be liable beyond their original contribution when they buy governance tokens that grant them mere voting rights in the DAO's governance, especially when the DAO has thousands of pseudonymous members. In this context, the members of the DAO have a status that is much closer to that of the shareholders of a limited company (*société anonyme, SA*) than that of the members of a simple partnership. Hence, when the founders who initiated the project and the core developers who developed the computer code exercise control over the DAO protocol, they can be viewed as the executive board managing the DAO. In such a situation, the decisions of the executive board (*i.e.*, the core developers and/or the founders with control over the DAO) need validation from the shareholders (*i.e.*, the members of the DAO) who vote to accept or refuse proposals.

It thus appears that Swiss substantive law does not have a legal regime adapted to maverick DAOs. Swiss law does not give those entities legal personality, nor does it provide their members with limited liability. Furthermore, the legal regime for simple partnerships is not adapted to govern the relationships among the members of maverick DAOs, between the members and the DAO itself, and between maverick DAOs and third parties. A legal solution for maverick DAOs should be found elsewhere than in the substantive law if one wishes to remedy this legal uncertainty.

When a legal situation has an international element, PIL provides rules that connect the legal situation with a particular state. Since maverick DAOs exist as inherently international entities, PIL rules could help connect DAOs to a foreign legal order which would determine their legal nature. Through the process of recognition of foreign companies, DAOs could potentially be granted legal existence in Switzerland by recognising them as foreign legal entities. Chapter 10 of the Private International Law Act (PILA)[36] is dedicated to the legal status of foreign companies in Switzerland. The first step in determining whether a foreign company legally exists in Switzerland is to determine whether it can be characterised as a company in the sense of Article 150 of the PILA. Both "organised associations of persons" and "organised assets" fall within this definition. "What can be characterised as a company is willingly very broad and includes all social combinations that have a social

35 Hess and Spielmann (n 30), 191–192, and cited references.

36 Swiss Private International Law Act of 18 December 1987 (SR 291).

organisation or that are at least organised as a whole."[37] Then, to legally exist and be subject to Swiss law, a foreign company must be validly constituted according to its *lex societatis*, which is the law under which the company is organised (Article 154 para. 1 PILA).[38] If the company fails to meet the constitution requirements of that law, Article 154 para. 2 PILA provides for a subsidiary connection to another legal order and the *lex societatis* becomes the law of the state where the company is actually administered. A company failing to meet the constitution requirements of the law of one of the states designated by Article 154 PILA cannot be recognised in Switzerland and does not legally exist in Switzerland.[39]

The founders and members of each maverick DAO can freely decide how to organise their entity by creating unique governance rules. Therefore, each maverick DAO must be individually analysed in order to determine whether it is sufficiently organised to qualify as a company within the meaning of Article 150 PILA. However, as seen above,[40] DAOs are economic and socially organised entities ruled by governance rules inscribed on a blockchain. Therefore, most DAOs are expected to be considered as sufficiently organised in the sense of Article 150 PILA.[41] If this is the case for a particular maverick DAO which seeks legal existence in Switzerland, it remains to be determined whether it is validly constituted according to its *lex societatis*. To answer this question, the law under which the DAO is organised must be determined. However, maverick DAOs are not organised according to a national law. They cannot be validly constituted according to the law of a state as there is no such connection. Thus, the main factor which connects a company to the state whose law governs its organisation leads to a dead-end when it comes to a DAO.

The next step is then to move on the subsidiary connecting factor for the *lex societatis* and determine the place where the DAO is actually administered. The authors consider that, as a rule, it is not possible to link the administration of a maverick DAO to a physical place. The management of DAOs is mostly

37 Swiss Federal Council, "Message concernant une loi fédérale sur le droit international privé (loi de DIP)," 10 November 1982, FF 1983 425 (translation by the authors). See Riva (n 2), 622.

38 See Florence Guillaume, "Article 154 PILA," in Andreas Bucher (ed), *Commentaire romand. Loi sur le droit international privé – Convention de Lugano* (Helbing Lichtenhahn 2011), para. 1.

39 Florence Guillaume, "Article 150 PILA," in Andreas Bucher (ed), *Commentaire romand. Loi sur le droit international privé – Convention de Lugano* (Helbing Lichtenhahn 2011), para. 18.

40 See *supra* chapter 2.1.

41 Riva (n 2), 625–627, analysed The DAO, Aragon Network, and dxDAO and came to the conclusion that all three DAOs were sufficiently organised to be considered companies in the sense of Art. 150 PILA.

organised in a flat hierarchy and conducted on-chain via their governance rule. When participants coordinate off-chain, it is usually done via online platforms such as GitHub and Discord, so much so that the administration of maverick DAOs cannot be linked to a geographical place. The only "place" of administration of maverick DAOs is the Internet and the blockchain itself, where votes pertaining to the governance take place. Any other attempt to anchor a maverick DAO in the territory of a state can only lead to a random and unpredictable result. Exceptions to this rule are possible when a maverick DAO has a particular connection with a state jurisdiction. For example, when participation in the DAO is restricted to a geographical location,[42] it can be concluded that the administration of the DAO is undertaken in this physical place. However, it is uncommon to restrict participation in a DAO on a geographical basis and exceptions are rare. Another reason to consider the administration of a DAO to be closely linked to a particular jurisdiction would be when the core developers or the founders at the origin of the project who have retained some control over the DAO are part of an organised entity such as a foundation or an association. In this case, it could be argued that the management of the DAO is conducted at the seat of that entity. However, when a DAO uses the services of a third company for certain administrative tasks but the strategic decision making remains with the DAO, one cannot consider that there is an actual administration within the meaning of Article 154 para. 2 PILA and that the DAO is anchored in the legal order at the seat of that company.[43]

Both criteria offered by Article 154 PILA fail to connect maverick DAOs to a state jurisdiction and no *lex societatis* can be identified. As connecting factors fail to link maverick DAOs to a particular state jurisdiction, no law can determine their legal regime. The recognition process fails insofar as it is not possible to determine if maverick DAOs have been validly constituted according to a foreign law. As a result, it is impossible for those "lawless" companies to legally exist in Switzerland. This leaves participants of maverick DAOs in a legally uncertain position, as those DAOs exist and function as entities but lack the legal recognition from states as legally existing companies. This situation highlights the disconnect between the connecting factors provided by law and the reality of activities being undertaken by individuals in the blockchain environment.

42 This is the case of NEDAO (see *supra* n 14).

43 For example, the Swiss company DAO.link was created to operate as an agent for The DAO in the physical world. The agency relationship that existed between the two entities was not sufficient to consider that The DAO was actually administered in Switzerland within the meaning of Article 154 para. 2 PILA and that Swiss law was the *lex societatis* of The DAO.

But does it make sense to determine the legal nature of a maverick DAO through any substantive law in the first place? One core characteristic of maverick DAOs is that they are created outside any legal framework. A second is that thousands of pseudonymous members can easily join them from anywhere in the world. The only framework that governs the interactions between those members is an immutable code that is distributed on a global network of computers. As maverick DAOs are not registered in the company register of a state, they do not rely on this traditional infrastructure to fulfill publicity requirements as required by law for some forms of companies.[44] Instead, they rely on the publicity and transparency offered by blockchain technology. Furthermore, the internal organisation of maverick DAOs is not dictated by rules of corporate law. Instead, the governance of maverick DAOs is solely defined by their code, relying on the "code is law"[45] doctrine.

To the authors' knowledge, there has yet to be a state that grants maverick DAOs legal existence within its jurisdiction even though "[i]t is in the interest of state jurisdictions, participants and third parties to allow maverick DAOs to exist as subjects of law."[46] In Switzerland, a solution based on the concept of functional equivalence[47] has already been proposed.[48] The understanding of the words "state" and "law" under Article 154 PILA could be extended to allow the code of maverick DAOs to be considered as their law and the online space as the state from which that law stems. According to this theory, the *lex societatis* of maverick DAOs would be their code. This way, maverick DAOs could be recognised in Switzerland as foreign companies validly constituted according to their code, which would be a comprehensive way to give them legal existence in Switzerland without having to introduce new legislation.[49]

---

44 *E.g.*, the company limited by shares of Swiss law acquires legal personality only through entry in the Swiss company register (Art. 643 para. 1 CO).

45 See *supra* n 20.

46 Riva (n 2), 632.

47 Some authors suggest that the principle of functional equivalence should be introduced in Switzerland to give smart contracts a legal scope without having to change provisions of substantive law. See Andreas Furrer and Luka Müller, "'Functional equivalence' of digital legal transactions – A fundamental principle for assessing the legal validity of legal institutions and legal transactions under Swiss law" (18 June 2018) <https://www.mme.ch/fileadmin/files/documents/MME_Compact/2018/180619_Funktionale_AEquivalenz.pdf> accessed 5 November 2021 [translation from Andreas Furrer and Luka Müller, "'Funktionale Äquivalenz' digitaler Rechtsgeschäfte – Ein tragendes Grundprinzip für die Beurteilung der Rechtsgültigkeit von Rechtsinstituten und Rechtsgeschäften im schweizerischen Recht" (*Jusletter*, 18 June 2018)].

48 Riva (n 2), 635–637.

49 Riva (n 2), 636.

At the international level, no international instrument (*e.g.*, a model law) with the purpose of harmonising the legal regime of DAOs has been proposed yet by the International Institute for the Unification of Private Law (UNIDROIT), the United Nations Commission on International Trade Law (UNCITRAL), or any other international organisation. However, the international working group COALA (Coalition of Automated Legal Applications), composed of experts from the legal and technological fields, is seeking to unify the legal regime of DAOs at the international level by proposing the COALA Model Law for Decentralized Autonomous Organizations (DAOs),[50] which is currently in the consultation phase. The Model Law for DAOs intends to define a flexible legal framework adapted to the characteristics of DAOs, which could be adopted by states in their national law. Any DAO complying with a set of best practices defined in the Model Law would be granted legal existence and acquire legal personality in the states having adopted the Model Law.[51]

2.3.2 Regulated DAOs

The innovations blockchain technology has brought to corporate governance and the rapid growth of the crypto economy have pushed a few states to bet on the use of blockchain technology in companies and believe that corporate structures could benefit, in terms of organisation, from digital architecture. In those jurisdictions, companies can now rely on blockchain technology to streamline internal processes. Those entities, referred to as regulated DAOs in the authors' terminology, use the blockchain infrastructure for their internal organisational structure and, at the same time, they are regulated by the corporate law of a state. While their code rules their governance, their legal nature and legal capacity are defined by corporate law. However, very few states have introduced legislation that grants legal status to DAOs. In states that offer the possibility of creating a DAO in accordance with the law, DAO members can take advantage of the protections afforded by the legal personality of the DAO, particularly with regard to the limitation of their personal liability. DAO members who want their entity to benefit from legal personality in one of those states must meet specific requirements of the law when constituting a DAO, for example registering the DAO in the state's company register.

---

50 The Model Law for DAOs is available at <https://coala.global/reports/#1623963887316-6ce8de52-e0a0> accessed 5 November 2021.

51 See Florence Guillaume and Sven Riva, "DAO, code et loi – Le régime technologique et juridique de la *decentralized autonomous organization*" (2021) 4 Revue de droit international d'Assas 206, available at <http://communication.u-paris2.fr/medias/RDIA_n4_2021.pdf> accessed 4 January 2022.

At the time of writing, three different jurisdictions, Malta, Vermont, and Wyoming have introduced the most prominent legislation allowing DAOs to be operated within a legal framework.[52] Malta adopted three bills on blockchain and cryptocurrency on 4 July 2018.[53] These bills set up a regulatory framework applicable to the blockchain environment and are collectively referred to as "The Digital Innovation Framework."[54] The Innovative Technology Arrangements and Services Act (ITAS) introduces the legal concept of the Innovative Technology Arrangement (ITA).[55] Smart contracts as well as DAOs can fall within the definition of an ITA.[56] Instead of granting ITAs legal personality, the Maltese legislator has created an agency relationship between an ITA and a person, who is referred to as the provider of Innovative Technology Services (ITS provider).[57] The ITS provider can be an individual or a legal entity with or without legal personality.[58] With this legal scheme, a DAO registered as an ITA does not acquire legal personality and does not have the capacity to sue or be sued. Even though a DAO registered as an ITA does not qualify as a legal entity, the DAO can rely on its agency relationship with the ITS provider to pursue activities in the mainstream economy. The ITS provider enters into contractual

52 A handful of other states have also passed DAO legislation. For example, the Marshall Islands modified their non-profit entities act in November 2021 to introduce non-profit DAO LLCs and non-profit DAO corporations. In the US state of Tennessee, a DAO bill heavily inspired from that of Wyoming's was signed into law in April 2022 to introduce DAO LLCs.

53 Welcome Center Malta, ICO & Crypto Regulation in Malta <https://www.welcome-center-malta.com/blockchain-services-in-malta/ico-crypto-regulation-in-malta/> accessed 5 November 2021.

54 Malcolm Falzon and Alexia Valenzia, "Malta," in Josias Dewey (ed), *Global Legal Insight – Blockchain & Cryptocurrency Regulation* (Rory Smith 2018), 378. See also Rachel Wolfson, "Maltese Parliament Passes Laws That Set Regulatory Framework For Blockchain, Cryptocurrency And DLT" (*Forbes*, 5 July 2018) <https://www.forbes.com/sites/rachelwolfson/2018/07/05/maltese-parliament-passes-laws-that-set-regulatory-framework-for-blockchain-cryptocurrency-and-dlt/#4e53149a49ed> accessed 5 November 2021.

55 Maltese Bill No C 689, Innovative Technology Arrangements and Services Act (2018) <https://legislation.mt/eli/cap/592/eng/pdf> accessed 5 November 2021.

56 First schedule, Art. 2 and Art. 8 para. 2 ITAS.

57 The preliminary report discussed the possibility of granting ITAs legal personality when they did not have an underlying ownership structure such as a corporation. However, the final bill does not deal with this issue. See Parliamentary Secretariat for Financial Services, Digital Economy and Innovation – Office of the Prime Minister, "Malta: A Leader in DLT Regulation" (2018), 18 <https://meae.gov.mt/en/Public_Consultations/OPM/Documents/PS%20FSDEI%20-%20DLT%20Regulation%20Document%20OUTPUT.PDF> accessed 5 November 2021.

58 Art. 10 para. 5 ITAS.

relationships on behalf of the DAO and is liable for the activities of the DAO since this person is identifiable by investors and authorities.[59]

The U.S. state of Vermont introduced a pioneering act that was signed into law on 28 August 2018,[60] which adds a new form of company to its legal order: the Blockchain-based Limited Liability Company (BBLLC).[61] A BBLLC is a DAO incorporated as a Limited Liability Company (LLC) in Vermont's jurisdiction. This act allows a DAO to validly enter into contractual relationships and protects its "owners, managers and blockchain participants from unwarranted liability."[62] General provisions related to LLCs apply to BBLLCs, as they are a specific form of LLC. The key innovation of that law is that the governance of a BBLLC can be fully or partially provided through blockchain technology, and votes regarding the operation and activities of a BBLLC can be recorded on blockchain-based smart contracts. The state of Vermont has seen in 2019 its first BBLLC incorporated as dOrg LLC,[63] which is believed to be the "first legal entity that directly references blockchain code as its source of governance."[64] Hence, BBLLCs are legal entities distinct from their members who are subject to a limited liability regime for the DAO's debts,[65] meaning that liabilities contracted by the DAO are not transferred to the members. The legal regime of BBLLCs gives DAOs for the first time the power to sue and be sued, to carry on business activities, and to enter into contractual relationships in their own name.

---

59 Paul Felice, "Presenting Innovative Technology Arrangements & Services Act" (*Finance Malta*, 18 July 2018).

60 Vermont Act No 205 (S.269), An act relating to blockchain business development <https://legislature.vermont.gov/Documents/2018/Docs/ACTS/ACT205/ACT205%20As%20Enacted.pdf> accessed 5 November 2021.

61 Title 11, Chapter 25, Subchapter 12 of the Vermont Statutes Online: Blockchain-Based Limited Liability Companies <https://legislature.vermont.gov/statutes/fullchapter/11/025> accessed 5 November 2021.

62 Propy, "Vermont S.269 (Act 205) and Blockchain-Based Limited Liability Companies (BBLLCs)" (*Hodl alert*, 31 August 2018) <https://www.hodlalert.com/2018/08/31/vermont-s-269-act-205-and-blockchain-based-limited-liability-companies-bbllcs/> accessed 5 November 2021.

63 Oliver Goodenough and Catherine Burke, "dOrg Launches First Limited Liability DAO" (*Gravel & Shea*, June 2019) <https://www.gravelshea.com/2019/06/dorg-launches-first-limited-liability-dao/> accessed 5 November 2021. See also Max Boddy, "DOrg LLC Purports to be First Legally Valid DAO Under US Law" (*Cointelegraph*, 12 June 2019) <https://cointelegraph.com/news/dorg-llc-purports-to-be-first-legally-valid-dao-under-us-law> accessed 5 November 2021.

64 Goodenough and Burke (n 63).

65 11 V.S.A. § 4042.

The DAO law of the U.S. state of Wyoming came into effect on 1 July 2021.[66] It introduced the DAO as a new form of company into Wyoming law.[67] A Wyoming DAO is an LLC whose articles of organization point to a DAO's smart contract used to manage and operate the company.[68] By making DAOs subject to the Wyoming Limited Liability Company Act in addition to the Decentralized Autonomous Organization Supplement,[69] the state of Wyoming took a similar approach than the state of Vermont. The particularity with Wyoming's Act is that it introduces a distinction between member managed and algorithmically managed DAOs.[70] The possibility to be managed by a manager, which is found in regular LLCs, is replaced for DAOs by the possibility to be managed by an algorithm.[71] Replacing a manager by an algorithm[72] is forward-thinking and a huge bet on technology. However, the exact meaning of the term "algorithm" is not defined in the law, and it is unclear whether a Wyoming DAO could be managed by an artificial intelligence[73] or by another DAO. Both cases would raise legal questions. For example, if the law allows a DAO to be

66 Wyoming Act No 73 (SF0038), Wyoming Decentralized Autonomous Organization Supplement <https://legiscan.com/WY/text/SF0038/id/2359146> accessed 5 November 2021.

67 Title 17, Chapter 31 of the Wyoming Statutes (W.S.) <https://advance.lexis.com/container/?pdmfid=1000516&crid=c52c919b-2865-4717-ad13-b9447da211be&config=00JAAzZmQ5YjBjOC1hNDdjLTQxNGMtYmExZi0wYzZlYWIxMmM5YzcKAFBvZENhdGFsb2cJAHazmy52H3XVa9c97KcS&ecomp=_sw_k&prid=8c598384-2227-4609-b3cf-07948922d930> accessed 5 November 2021. The law also refers to DAOs as Limited liability Autonomous Organizations (LAOs).

68 W.S. §17-31-106 (b).

69 W.S. §17-31-103.

70 W.S. §17-31-104 (e).

71 See Shawn Bayern, "The Implications of Modern Business-Entity Law for the Regulation of Autonomous Systems" (2015) 19 Stanford Technology Law Review 93. This author argues that LLC laws of various U.S. states implicitly permit LLCs to exist without any members while being managed by an artificial intelligence. The state of Wyoming has taken the step of expressly introducing in its law the possibility for an LLC to be managed by an algorithm.

72 The legal nature of the agency relationship between an algorithmically managed Wyoming DAO and the members of the DAO is not defined in the law and remains unclear.

73 Some authors have already considered the possibility of a traditional company being run by an algorithm or artificial intelligence. The latter could either help the members of the company to make decisions or even replace the members in a corporate body. For example, an artificial intelligence could sit on the board of directors and be granted decision rights. See Florian Möslein, "Robots in the boardroom: artificial intelligence and corporate law," in Woodrow Barfield and Ugo Pagallo (eds), *Research Handbook on the Law of Artificial Intelligence* (Edward Elgar 2018), 649; Shawn Bayern and others, "Company Law and Autonomous Systems: a Blueprint for Lawyers, Entrepreneurs, and Regulators" (2017) 9 Hastings Science and Technology Law Journal 135.

managed by an autonomous algorithm, does the algorithm have the power to contractually bind the DAO to third parties?[74] And while Wyoming DAO members benefit from limited liability on the same basis as other LLCs,[75] it is unclear how some aspects pertaining to the scope of the liability are affected by the DAO structure, in particular when the DAO is managed by an algorithm.[76] Furthermore, while DAO members are subject to the LLC legal framework at the state level, some Wyoming DAO token holders may be subject to federal securities law and other unexpected federal regulations.[77] Nonetheless, a DAO organised under Wyoming law has the capacity to sue and be sued in its own name, and the power to undertake business activities and to enter into contractual relationships.[78]

Regulated DAOs do not differ much from any other corporate form. The legal path chosen by those three legislators has been to introduce in their substantive law a new corporate form which relies on blockchain technology. However, none of the existing DAO regulations integrate provisions addressing the legal status of maverick DAOs. There are no rules of PIL that allow for the recognition of a DAO created according to the provisions of the law of another state either. Quite the opposite, Wyoming's DAO law explicitly forbids the recognition of foreign DAOs, without defining what is meant by "foreign DAOs."[79] This legal provision seems odd as PIL should allow corporate entities to enter into cross-border commercial relationships by recognising the legal nature of foreign companies as defined by the law under which they are constituted. By forbidding foreign DAOs to be issued a certificate of authority without specifying which types of entities are actually covered, this legal provision introduces legal uncertainty as to whether a DAO organised for example as a Vermont BBLLC and validly constituted according to that law could lawfully undertake business activities in the state of Wyoming. It is thus unclear if a Vermont BBLLC would be considered a foreign DAO or a foreign LLC in that state.

74 This would lead to the emergence of "software-negotiated contracts" as described by Shawn Bayern, "Artificial intelligence and private law," in Woodrow Barfield and Ugo Pagallo (eds), *Research Handbook on the Law of Artificial Intelligence* (Edward Elgar 2018), 144, 150–152.

75 W.S. §17-29-304.

76 Andrew Lom and Racheal Browndorf, "Wyoming to Recognize DAOs as LLCs" (*Regulation tomorrow*, 30 April 2021) <https://www.regulationtomorrow.com/us/wyoming-to-recognize-daos-as-llcs/> accessed 5 November 2021.

77 Lom and Browndorf (n 76). Vermont BBLLC token holders could also be faced with this uncertainty as both forms of companies are subject to U.S. federal law.

78 W.S. §17-29-105.

79 W.S. §17-31-116.

Ironically, a validly constituted Vermont BBLLC would most certainly be recognised and be allowed to undertake business activities in Switzerland. A regulated DAO would indeed qualify as a company as defined under Article 150 of the PILA, even though DAOs cannot be constituted under Swiss law. Such DAOs are organised under the law of a specific state and their *lex societatis* can therefore be identified. A regulated DAO would legally exist in Switzerland, without having to complete any particular formalities, provided it fulfils the publicity or registration requirements of the law of the state under which it is organised (Article 154 para. 1 of the PILA).[80]

These three models of DAO legislation show that it is possible to give legal status to DAOs, under certain conditions, by allowing them to submit to a legal framework. This legislation defines the legal nature of the relationships among the members of a DAO and between the members and the DAO itself, and allows the economic and social activities of those DAOs to have a legal scope. They also determine the legal nature of the agency relationships between DAOs and their representatives, whether it is with their members, managers or agents. However, regulated DAOs remain actors of the crypto environment. By existing simultaneously in a state jurisdiction and on the blockchain, regulated DAOs are a hybrid-type of company. While a regulated DAO is one single entity under the law, there are actually two very distinctive parts to a regulated DAO: the corporate body (*e.g.*, the LLC) which gives legal substance to the entity, and the DAO (*i.e.*, the code) which structures the organisation of the entity. The two parts of the entity are linked by corporate law, but they are subject to very different sets of rules. The entity as a whole is subject to corporate law and is under the jurisdiction of the state where it is registered or incorporated, or under which law it is constituted or organised. There is a real link between that state and the entity through its corporate body. This link is materialised, in the three DAO laws discussed above, by the registration of the entity in a company register, and by requiring that the DAO be represented by at least one person who has some form of liability for the actions of the DAO. For its part, the DAO is governed by its code and can only be managed in accordance with its code. There is a real link with the blockchain, which is materialised by the registration of the DAO in the ledger. This characteristic of regulated DAOs – two distinct parts of a single entity – is not found in maverick DAOs. Indeed, maverick DAOs are not attached to the legal system of a particular state and therefore do not have a corporate body subject to corporate law. Only regulated DAOs have an existence that materialises both on- and off-chain. These

80 Riva (n 2), 629–630. See also *supra* chapter 2.3.1.

features, which relate to the organisational structure of DAOs, must be considered in the event of a dispute involving a DAO.

3 Jurisdiction for Disputes Involving DAOs

As with other entities, DAOs are subject to disputes among their members, between the DAO and its members, and with third parties. Even if the architecture of smart contracts and the blockchain allow DAOs to be programmed in order to reduce the number of disputes within the entity and with third parties, not all disputes can be prevented from occurring. Disputes involving a DAO are in principle international in scope. By functioning on public blockchains, DAOs are international entities by nature, whether they are governed by a national law or not. In order to determine in which state a DAO can sue or be sued, the rules of PIL must be applied.

PIL aims to provide the legal certainty necessary for the development of international relations between individuals. The localisation of the subject of the dispute and the parties themselves with connecting criteria is at the core of the method of PIL. The aim is to coordinate the legal orders by identifying the state with which the activity and the parties have the closest connections or, at least, sufficient connections.[81] A state will agree to provide the protection of its courts when the subject of the dispute or one of the parties has sufficient connections with its territory. Legal certainty is thus granted by the adoption of PIL rules which determine with certainty the courts that have jurisdiction over a dispute. The application of the rules of jurisdiction to disputes involving a DAO raises difficulties with regard to the use of connecting factors. To illustrate this issue, two types of disputes will be examined hereafter: those relating to the governance of DAOs, which are likely to fall under corporate law if a DAO qualifies as a company, and disputes between a DAO and a third party arising from a business relationship that is of a contractual nature. Other types of disputes will not be considered (*e.g.*, administrative disputes between a DAO and a state).

To this end, we will first establish that, although smart contracts aim to create a rigid framework where disputes are minimal, they fail to prevent all disputes from occurring (3.1). We will then differentiate disputes into two categories and analyse whether connecting factors of PIL allow the linking of those disputes to the courts of a state. We will first analyse disputes related to the governance of DAOs and try to locate them using connecting factors.

81 Andreas Bucher, *La dimension sociale du droit international privé – Cours général* (ADI-Poche 2011), 48–65.

Maverick DAOs and regulated DAOs will be analysed separately, as regulated DAOs are connected to a legal order (3.2). Then, we will analyse disputes of a contractual nature and seek to determine whether it is possible to localise the legal relationship at the place of the DAO, the other party, or the performance of the contract (3.3). With the difficulty to localise disputes involving DAOs using connecting factors of PIL, we will introduce universal jurisdiction as an alternative way to connect a dispute to a state jurisdiction (3.4). We will then consider the extent to which blockchain technology is an impediment to the enforcement of court decisions (3.5). This analysis will lead us to acknowledge that state courts do not have the proper tools to guarantee justice with disputes involving DAOs (3.6).

3.1 *Smart Contracts as a Non-foolproof Technology*

DAOs rely on smart contracts to enter into contractual relationships with third parties. By having their commitments coded on a smart contract, DAOs and their contractual partners are guaranteed a perfect performance of all contractual obligations. As smart contracts are recorded in the ledger of a blockchain, which is tamperproof, they are also immutable. A smart contract that has already been executed cannot be unilaterally deleted, and a smart contract that has not yet been executed cannot be unilaterally modified. Therefore, smart contracts have been advertised as being a fail-proof way to enter into contractual relationships, especially when contracting with unreliable third parties.[82] The code automatically executes the terms of the contract when the programmed conditions are met. This leads to the perfect execution of the contract, potentially removing all needs for dispute resolution between the parties,[83] greatly reducing transaction costs.[84] In sum, the execution of a contractual obligation in the blockchain environment is ensured by technology, making courts redundant, at least in theory.

However, as with any human-driven technology, smart contracts can also deliver unexpected results. Mistakes can occur in the process of converting the

82 Wulf A. Kaal and Craig Calcaterra, "Crypto Transaction Dispute Resolution" (2017–2018) 73 The Business Lawyer 109, 110; Rikka Koulu and Kalle Markkanen, "Conflict Management for Regulation-Averse Blockchains?," in Rosa Maria Ballardini, Petri Kuoppamäki and Olli Pitkänen (eds), *Regulating industrial Internet through IPR, Data Protection and Competition Law* (Wolters Kluwer 2019), 382.

83 See Kevin Werbach and Nicolas Cornell, "Contracts ex Machina" (2017) 67 Duke Law Journal 313, 352–363.

84 See De Filippi and Wright (n 13), 80–81.

terms of the legal contract into the code of the smart contract.[85] Errors in the code or bugs, as well as unforeseen circumstances that were not programmed in the smart contract, can lead to unwanted outcomes in its execution. A conflict can also arise from differences in the interpretation of the smart contract's code, for example at the time of verification by an external source (so-called "oracle") of factual elements whose occurrence in the physical world triggers the performance of the smart contract. A party to a smart contract can also feel aggrieved when the smart contract executes as planned, but the result contravenes principles of fairness and justice. In sum, the fact that smart contracts run automatically does not eliminate the risk of litigation.[86]

DAOs also completely rely on the architecture of smart contracts for their operation and management. Their internal governance is encoded on smart contracts which contain the rules dictating the relationships among the members of the DAO and defining its governance structure. By relying on the code and removing human involvement in the execution process, smart contracts could be seen as the ultimate solution to improve corporate governance efficiency. Internal processes are automated and transparent, reducing monitoring costs and the costs of agent supervision.[87] However, what is encoded in the smart contract is not necessarily fair and legally just. Even when the code works as planned, disputes might appear among the members of a DAO. Such conflicts might occur when a minority shareholder feels that their rights were violated by majority shareholders. Furthermore, DAOs are also prone to bugs in the smart contracts defining their governance structure and operations. The more complex a DAO structure is, the more at risk it is to encounter such

85 Legal contracts are contracts that are legally binding upon the parties. See *infra* chapter 3.3.

86 Same opinion: Orna Rabinovich-Einy and Ethan Katsh, "Blockchain and the Inevitability of Disputes: The Role for Online Dispute Resolution" (2019) 2 Journal of Dispute Resolution 47; Amy J. Schmitz and Colin Rule, "Online Dispute Resolution for Smart Contracts" (2019) Journal of Dispute Resolution 103, 104; Pietro Ortolani, "The impact of blockchain technologies and smart contracts on dispute resolution: arbitration and court litigation at the crossroads" (2019) 24 Uniform Law Review 430, 438; Darcy W.E. Allen, Aaron M. Lane and Marta Poblet, "The Governance of Blockchain Dispute Resolution" (2019) 25 Harvard Negotiation Law Review 75, 81–82; James Metzger, "The Current Landscape of Blockchain-Based Crowdsourced Arbitration" (2019) 19 Macquarie Law Journal 81; Kaal and Calcaterra (n 82), 142; Kevin Werbach, "Trust, But Verify: Why the Blockchain Needs the Law" (2018) 33 Berkeley Technology Law Journal 487; Koulu and Markkanen (n 82), 381; Marc Clément, "Smart Contracts and the Courts," in Larry A. DiMatteo, Michel Cannarsa and Cristina Poncibò (eds), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (Cambridge University Press 2020), 271.

87 Kaal (n 19), 11.

problems. The example of "The DAO" showcases how a flaw in the code can lead to a DAO's downfall.[88]

Now that we have established that smart contracts cannot prevent all disputes from occurring, and that DAOs can be prone to internal conflicts (between a DAO and its members or among its members) as well as external conflicts (between a DAO and third parties), it remains to be determined whether those disputes can be resolved by state courts. The key issue is to establish whether existing connecting factors are able to link disputes involving DAOs to a state and whether the PIL rules of that state grant jurisdiction to its courts over those disputes. If this is not the case, actors of the blockchain ecosystem could find themselves in situations of denial of justice.

3.2 *Connecting Disputes Related to the Governance of DAOs*

Corporate law deals with disputes related to the governance of companies. Those disputes include proceedings on the validity of the constitution, the nullity or the dissolution of the company, or the validity of the decisions of its organs. As they pertain to the company's internal structure, those disputes have close links with the place of incorporation and, to some extent, also with the place of administration of the company. The first criterion anchors the company to the state under which it is constituted or organised. The registered office of the company is usually situated in this country. The second criterion anchors the company in the state in which it is managed. Those places correspond, in principle, to the place of the seat(s) of the company.

Taking the Swiss legal order as an example, Swiss PIL links disputes of corporate law to the Swiss courts of the seat of the company (Article 151 para. 1 of the PILA). The seat of a company is deemed to be located at the place designated in the bylaws or articles of association (statutory seat, registered office), or at the place where the company is administered in fact (administrative seat) (Article 21 para. 2 of the PILA). When the action is aimed towards a specific individual, for example a shareholder, a member of the company, or any other liable person according to corporate law, close connections also exist with the domicile or habitual residence of that person and there is a forum at that place (Article 151 para. 2 of the PILA). We will base our analysis on the rules of Swiss PIL which grant jurisdiction to Swiss courts in corporate law matters in order to link disputes pertaining to the governance of DAOs to a legal order. Such rules can be found in the PILA and the Convention on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters of

88 See *supra* chapter 2.1.

30 October 2007 (the "Lugano Convention").[89] This will allow us to determine whether Swiss courts offer their protection for those kinds of disputes. We will examine this issue first in relation to maverick DAOs (3.2.1) and then in relation to regulated DAOs (3.2.2).

3.2.1 Maverick DAOs

The following observations apply to maverick DAOs that qualify as companies within the meaning of PIL.[90] In this case, a dispute over the governance of the DAO can be characterised as a corporate law matter and is therefore prone to falling under the jurisdiction of the Swiss courts of the seat of the DAO (Article 151 para. 1 of the PILA).[91]

However, maverick DAOs do not have a seat: there is neither a place of incorporation nor any place of administration that could point to a state. Maverick DAOs cannot be linked to a state jurisdiction because they are not constituted or organised under the law of a state and their members are pseudonymous.[92] Those DAOs are simply launched on a blockchain and profit from the blockchain's infrastructure to register their "bylaws" (*i.e.*, their code) and to become a publicly visible entity. It is very unlikely that a maverick DAO would designate a seat in its code. Thus, the criterion of the statutory seat or registered office fails to link maverick DAOs to a state. Likewise, there is no physical place of administration of maverick DAOs and the criterion of the administrative seat fails to create any link with a state. As they are comprised of a community of pseudonymous members who jointly manage the operations of the entity through online platforms (*e.g.*, GitHub), the criterion of the administrative seat can only point to the Internet or the blockchain itself.

In some exceptional cases, membership to a maverick DAO can be geographically limited. When it can be determined with certainty that a majority of the members of a maverick DAO reside in one state, the place of administration of the maverick DAO may be anchored in that state.[93] For example, the members of NEDAO must be residents of the canton of Neuchâtel, Switzerland.[94] In case

89 SR 0.275.12; [2007] OJ L 339/3.

90 In Switzerland, this means that the concerned DAO qualifies as a company in the sense of Art. 150 of the PILA. See *supra* chapter 2.3.1.

91 It should be noted that if the seat of the DAO is in Switzerland, Art. 22 para. 2 of the Lugano Convention applies exclusively to establish the jurisdiction of the Swiss courts for actions falling within its scope. In this case, Art. 151 para. 1 of the PILA is used to determine the local jurisdiction of the Swiss courts.

92 See *supra* chapter 2.3.1.

93 See *supra* chapter 2.3.1.

94 See *supra* n 14.

of a dispute of corporate law matter involving NEDAO, Swiss courts – and more precisely the courts of Neuchâtel – could have jurisdiction over the case based on the criterion of the place of administration. However, Swiss courts would have to determine whether NEDAO can be a party to the proceedings. This is very unlikely, as no law grants NEDAO legal capacity, *i.e.*, the capacity to sue or be sued. Likewise, when the core developers of a DAO or the founders at the origin of the project are part of an organised entity such as a foundation or an association, the courts of the seat of that entity could have jurisdiction over the dispute since it can be considered that the DAO is administered in fact at this place, provided at least that they can exercise some control over the governance of the DAO.[95]

With the exception of such special cases, if we consider that disputes related to the governance of a DAO are matters of corporate law, connecting factors of Swiss PIL fail to link those disputes to Switzerland. The same conclusion can be reached for other state jurisdictions, as even though the connecting criteria for determining the jurisdiction of their courts are not necessarily identical to those in Switzerland, they are very similar. It is therefore likely that they will also fail to establish a sufficient link with maverick DAOs to give jurisdiction to their courts. This situation leads to a negative conflict of jurisdiction, meaning that no state has jurisdiction over issues pertaining to the governance of a maverick DAO. And even if a maverick DAO could be located in a particular state, it is unlikely that it could be a party to the proceedings as it would probably not have the right to sue or be sued. This leaves members of maverick DAOs with no legal recourse when their rights are infringed. Weaker members such as minority shareholders are at particular risk of denial of justice.

Furthermore, when a particular member of a maverick DAO is liable for damages sustained by the DAO, which is a matter falling within the scope of corporate law, the courts of the place of domicile or habitual residence of that member may have jurisdiction over the matter (Article 151 para. 2 of the PILA).[96] However, the members of maverick DAOs are usually pseudonymous and it is virtually impossible to identify them to determine the place of their domicile or habitual residence. In this case, the DAO that suffered the damage and the other members would have no place to engage legal proceedings.

From the authors' point of view, all connecting criteria of PIL fail to link disputes of corporate law involving maverick DAOs to a state in order to find a forum for actions related to the governance of those DAOs. This is not a surprise as maverick DAOs are constituted outside any legal framework. They do

95 See *supra* chapter 2.3.1.

96 The international jurisdiction of Swiss courts is actually determined by Art. 2 para. 1 of the Lugano Convention when the defendant is domiciled in Switzerland. In this case, Art. 151 para. 2 of the PILA is used to determine the local jurisdiction of the Swiss courts.

not have a *lex societatis* governed by the rules of law, the only place where they are registered is on the blockchain, their management happens exclusively on the blockchain, and their activities are mainly carried out in the environment of the blockchain. Their members also challenge existing connecting criteria thanks to the pseudonymity they enjoy from operating on the blockchain. This shows that existing rules of PIL are ineffective in this transnational environment where individuals benefit from pseudonymity.

When dealing with maverick DAOs, connecting criteria are unsuitable for linking a dispute to the territory of a state using the seat of the DAO or the domicile or habitual residence of its members. It follows that disputes related to the governance of maverick DAOs is beyond the reach of state justice. This shows how blockchain technology is defying the purpose of PIL, which is to link legal situations to a state,[97] and creates a serious risk of denial of justice for individuals taking part in a maverick DAO and for maverick DAOs themselves. This unfortunate situation could only be improved if connecting criteria could take into consideration the specificity of the crypto environment.

3.2.2 Regulated DAOs

We will now examine whether the rules of PIL allow regulated DAOs to be linked to a state when they are involved in a dispute related to their governance. The analysis is different from that of maverick DAOs since regulated DAOs are a hybrid-type of company which exist simultaneously in a state jurisdiction and on the blockchain.[98] The authors assume that regulated DAOs that are validly constituted according to their *lex societatis* qualify as companies within the meaning of PIL.[99] As such, a dispute over the governance of a regulated DAO can be characterised as a corporate law matter.

Regulated DAOs have commonalities with maverick DAOs by carrying out their activities mainly on the blockchain. However, their situation is fundamentally different from that of maverick DAOs in that they do have a *lex societatis* governed by the rules of law. Regulated DAOs are not only registered in the ledger of a blockchain, but also in a register held by a state. Existing DAO laws require that regulated DAOs be connected to their state of incorporation, whether by requiring the registration of the DAO in a company register, by connecting the DAO to a registered company, or by requiring that the DAO be

97 This is also the case for the Internet. Many years of case law have been necessary to adapt the interpretation of connecting criteria in order to be able to locate legal situations emerging from the Internet. See Dan Jerker B. Svantesson, *Solving the internet jurisdiction puzzle* (Oxford University Press 2017), 91–112, who outlines a history of Internet jurisdiction.

98 See *supra* chapter 2.3.2.

99 See *supra* chapter 2.3.2.

represented by at least one registered person. Additionally, it can be assumed that maverick DAOs are validly constituted or organised under the law of the state which provides them with a legal framework. This allows the criterion of the incorporation to establish a link between a regulated DAO and a specific state. This way, even if the activities of a regulated DAO are carried out exclusively on the blockchain and its members are pseudonymous, there is always a link between the DAO and a state jurisdiction. Regulated DAOs can be considered as having a seat at the place of their statutory seat or registered office. Therefore, the courts of the states having adopted DAO legislation – such as Malta, Vermont, and Wyoming – may have jurisdiction over disputes related to the governance of DAOs that are registered or incorporated in their jurisdiction, or that are constituted or organised under their law.

As regards the administration of regulated DAOs, it could be argued that (at least) some of them are managed exclusively on the blockchain, just as their maverick counterparts. Such regulated DAOs do not have an administrative seat. However, it cannot be totally excluded that some regulated DAOs may also be in part managed off-chain, either on online platforms or in person. In the latter case, the place of administration could create a link between the DAO and a specific state. Swiss courts could thus have jurisdiction for disputes related to the governance of a regulated DAO if the place where it is administered in fact is located in Switzerland. However, this situation is very unlikely, because the jurisdiction of Swiss courts could be exercised in this case only if the DAO had no statutory seat or registered office.[100] But other states may offer the protection of their courts when a regulated DAO is administered on their territory.

In the states where a regulated DAO must have a registered manager or agent, the domicile or place of residence of the manager or agent (or the place of its establishment) creates an additional link with a state jurisdiction. Under most laws with such a requirement, the registered representative of a company must reside in the company's state of incorporation as it serves as a link between the state and the company. In this case, the domicile or place of residence of the registered representative blends with the place of the statutory seat or registered office. It can be concluded that the links with that place are particularly strong. When a regulated DAO must have a registered representative, it can be expected that the jurisdictional rules of the state where the representative is located will grant jurisdiction to its courts for all disputes related

100 See Art. 151 para. 1 and Art. 21 para. 2 of the PILA.

to the governance of the DAO, especially if the representative is domiciled in the DAO's state of incorporation.

In some instances, members of a company are liable for damages suffered by the company or other members. In that case, a link with the domicile or place of residence of the liable member exists and the courts of that state may have jurisdiction over the dispute. Contrary to maverick DAOs whose members are usually all pseudonymous, it is very likely that at least some members of regulated DAOs are registered in a state company register, making their personal information known and circumventing pseudonymity of the blockchain. This allows connecting factors of PIL to point to a known jurisdiction. Therefore, proceedings can easily be opened against a registered liable member. However, if the dispute is with a member who is not registered, that member potentially still benefits from the pseudonymity of the blockchain, which prevents the establishment of a link with a specific state based on personal jurisdiction. The only available forum would then be at the place of the statutory seat or registered office of the DAO, and eventually at the place of its administrative seat. But with an unknown defendant, the scope of the proceedings would be very limited.

Some laws may allow for a regulated DAO to be managed by an algorithm. This is potentially the case in the U.S. state of Wyoming.[101] If an algorithm were to be liable for damages of corporate law nature,[102] one may wonder whether the algorithm could be located in a particular state and, if so, whether locating the algorithm would give sufficient links with a state to grant jurisdiction to its courts. The criterion of the domicile or habitual residence is the one which is usually used to establish jurisdiction for an action against a manager of a company.[103] The application of this connecting factor to a managing algorithm would of course fail to give a convincing result. However, in the case of an algorithm, other connecting factors such as the place of the server(s) could

101 See *supra* chapter 2.3.2.

102 To the authors' knowledge, there is no law to date recognising the capacity of an algorithm, an artificial intelligence, or a robot to sue or to be sued in its own name. However, this issue has already been addressed by several legal scholars. See *e.g.*, Woodrow Barfie ld and Ugo Pagallo, *Law and Artificial Intelligence* (Edward Elgar 2020), 60–76; Roger Michalski, "How to Sue a Robot" (2018) 5 Utah Law Review 1021; Robert van den Hoven van Genderen, "Legal personhood in the age of artificially intelligent robots," in Woodrow Barfield and Ugo Pagallo (eds), *Research Handbook on the Law of Artificial Intelligence* (Edward Elgar 2018), 213.

103 See *e.g.*, Art. 151 para. 2 of the PILA.

prove to be adapted.[104] If it is possible to establish that the algorithm is located in a different place than the statutory seat or registered office of the DAO, it remains to be determined whether the connection is sufficiently strong to grant jurisdiction to the courts of that place for damages of corporate law. This issue can be dealt with differently from one state to another since each state is free to determine when it offers the protection of its courts. From the authors' point of view, the state of the place of incorporation of the DAO should probably grant jurisdiction to its courts if it is possible to hold an algorithm liable for damages under its legislation.

As we have seen above, while some connecting factors of PIL fail to link disputes of corporate law involving regulated DAOs to a state, the criterion of the place of incorporation seems to be appropriate to locate such disputes in the state of the *lex societatis*. This systematic fall back on the place of the statutory seat or registered office of the DAO shows that PIL has difficulties locating conflicts related to the governance of regulated DAOs. In some cases, the structure of the blockchain even prevents the identification of the defendant. In those instances, linking the dispute to the courts of a state is proven to be superfluous.

In theory, jurisdiction of the courts of the state where the DAO is registered or incorporated, or under which law it is constituted or organised, seems to be natural. However, in practice, things are more complicated than it seems at first glance. Jurisdiction of the courts of the state of the statutory seat or registered office of a regulated DAO should cover all disputes related to the governance of the DAO. Given the hybrid nature of regulated DAOs, some of those disputes will be governed by the rules of corporate law and others by the rules of code. The entity as a whole is indeed subject to corporate law, but the DAO part is also governed by the code on the blockchain.[105] This feature actually brings a great limitation to the scope of the jurisdiction of state courts. While the corporate body (*e.g.*, the LLC) falls under the jurisdiction of state authorities, the DAO as such is not directly under the jurisdiction of state authorities. In general, a payment in cryptocurrencies or other actions to be performed on-chain can only be triggered when the majority of the DAO's members agree to it. No one can force a DAO to act in a certain way if it is contrary to

104 The connecting factor of the location of the server carrying a website has already been used in the field of tort law. See *e.g.*, Dan Jerker B. Svantesson, *Private International Law and the Internet* (3rd edn, Wolters Kluwer 2016), 468–469. However, this criterion would not work when the algorithm is "located" on a public blockchain, because such a blockchain is inherently transnational.

105 See *supra* chapter 2.3.2.

its code. As the community of members is pseudonymous and each member can potentially be physically outside the personal jurisdiction of the state of incorporation of the DAO, there is a risk that the DAO will not comply with a request or decision made by the authorities of that state. A friction can therefore exist between what the DAO must do legally, and what state authorities can actually enforce upon the DAO. This can potentially put a huge burden of liability on the registered manager(s) or agent(s), or the registered member(s) of the regulated DAO.

It can be concluded at this point that while it may appear relatively simple, at first glance, to create a connection between a regulated DAO and a state, there is nevertheless a serious risk of denial of justice for disputes related to the governance of regulated DAOs. This risk is all the greater because, even if it is possible to obtain a decision from a state court, state authorities will often be powerless when the use of force is necessary to enforce the decision. However, the state of incorporation may exercise a direct coercive power on a regulated DAO which does not comply with requests or decisions made by its authorities by revoking its legal status. The main difference between a regulated DAO and other forms of company is that a regulated DAO that would lose its legal status would simply convert into a maverick DAO. Even if it drops its corporate body, an ex-regulated DAO can keep operating as an economic or social entity and pursue its activities in the blockchain environment.

3.3 *Connecting Disputes of a Contractual Nature Involving DAOs*

DAOs are entities that are best suited for doing business in the blockchain environment. The majority of their activity is carried out on the blockchain through smart contracts, of which two types can be distinguished.[106] The first are smarts contracts that are linked to an underlying legal contract where the smart contract serves to perform one or more contractual provisions, or where the smart contract is a reproduction of the legal contract which is legally binding upon the parties. The second are smart contracts that are the legal contract themselves and no link exists with an underlying contract. We will hereafter only consider the second type of smart contracts.

106 See Florence Guillaume, "L'effet disruptif des smart contracts et des DAOs sur le droit international privé," in Alexandre Richa and Damiano Canapa (eds), *Droit et économie numérique* (Stämpfli 2021), 35, 44; Blaise Carron and Valentin Botteron, "How smart can a contract be?," in Daniel Kraus, Thierry Obrist and Olivier Hari (eds), *Blockchains, Smart Contracts, Decentralised Autonomous Organizations and the Law* (Edward Elgar 2019), 101, 111–114.

Assuming that a relationship between a DAO and a third party defined by a smart contract can be qualified as a contractual relationship in the legal sense,[107] it is possible to use connecting criteria provided for by the rules of PIL to connect the contractual relationship to a state jurisdiction. The connecting factors used in contractual matters refer either to the location of the parties or to the location of the contractual relationship itself. For example, under Swiss PIL, Swiss courts have jurisdiction to hear disputes arising from a contract primarily when the defendant has its domicile or, failing that, its habitual residence in Switzerland (Article 112 para. 1 of the PILA). In the case of a company, the seat is deemed to be the domicile (Article 21 para. 1 of the PILA), which is located at the place designated in the bylaws or articles of association (*i.e.*, the statutory seat or registered office), or failing that, at the place where the company is administered in fact (*i.e.*, the administrative seat) (Article 21 para. 2 of the PILA). There are other fora in contractual matters, such as the forum at the place of performance of the contract. The Swiss courts have jurisdiction when the characteristic obligation of the contract is to be performed in Switzerland (Article 113 of the PILA). Similar criteria are found in the Lugano Convention, which applies in contractual matters when the defendant is domiciled in Switzerland or another contracting state of the Lugano Convention (Article 2 para. 1 and Article 5 para. 1 of the Lugano Convention). We will hereafter consider how the connecting criteria of Swiss PIL granting jurisdiction to Swiss courts in contractual matters can be applied to disputes between a DAO and a contracting party by analysing the means to locate the DAO (3.3.1), the other party (3.3.2), and the performance of the contract (3.3.3).

3.3.1 Location of the DAO

The first rule of jurisdiction to be considered in contractual matters is the forum of the domicile of the defendant (Article 112 para. 1 of the PILA).[108] When the defendant in a dispute over the execution of a smart contract is a DAO, the rules on determining the seat of the DAO, as illustrated in the last chapter, apply in the same way to connect the dispute to the domicile of the defendant.[109] However, it is not possible to establish the domicile of a maverick DAO in a state for the purpose of determining a forum. It is very unlikely that a maverick

107 See *supra* n 8.

108 For the sake of simplicity, we will only refer to the PILA even though the international jurisdiction for disputes of contractual matters is actually determined by Art. 2 para. 1 of the Lugano Convention when the defendant is domiciled in Switzerland. In this case, Art. 112 para. 1 of the PILA is used to determine the local jurisdiction of the Swiss courts.

109 See *supra* chapter 3.2.

DAO would designate in its code a statutory seat or registered office in a state jurisdiction. Maverick DAOs do not have an administrative seat either: they are mostly governed on the blockchain and on online platforms. One exception is when membership in a maverick DAO is geographically restricted to a state – for example to the residents of the canton of Neuchâtel –, in which case the maverick DAO could be anchored in that state. The reason is that the members administrating the DAO would be *de facto* residents of that state.[110] From the authors' point of view, this can be considered as a sufficient link to acknowledge the existence of a *de facto* seat of the maverick DAO in that state. However, even if a dispute of a contractual nature involving a maverick DAO can be linked to a state, it is unlikely that the DAO would be a party to the proceedings, as no law grants maverick DAOs the capacity to sue and be sued in their own name. In addition, there is a significant risk, as the law stands, that a state court would consider that a maverick DAO does not have the power to enter into a contractual relationship and be entitled to rights and obligations of any kind in its own name.

For their part, regulated DAOs can be linked to a state using the criterion of the statutory seat or registered office. This criterion successfully locates the seat of a regulated DAO in the state where it is incorporated or registered. It may therefore be possible to sue a regulated DAO in the forum of its domicile in that state. As for the administrative seat, it would not systematically succeed at linking regulated DAOs to a state since they can be governed on-chain as well as off-chain in a physical location. When regulated DAOs are exclusively governed online, the criterion of the place of administration points to the Internet or the blockchain rather than to a state jurisdiction. However, when regulated DAOs are not managed online, it is possible to identify a place of administration in a specific state. The courts of the state where the DAO's administrative seat is located may have jurisdiction. In sum, by being registered in a state, regulated DAOs can generally always be located, even if they are exclusively administered online.

3.3.2 Location of the Other Party

When contracting on the blockchain, DAOs can be confronted with two different types of contracting parties: on-chain and off-chain actors. If a DAO bound under a smart contract suffers economical damage due to the non-execution or improper execution of the contract, locating the other party could open

110 See *supra* chapter 2.3.1.

a forum at the domicile or habitual residence of the defendant, potentially giving jurisdiction to the courts of that state.[111]

On-chain actors are third parties acting on the blockchain, including individuals or DAOs, who can only be identified by their wallet address (*i.e.*, their public key).[112] As on-chain actors act pseudonymously in the blockchain environment, it may be impossible to locate their domicile or habitual residence, or their seat. It can therefore be very difficult if not impossible to subject them to the jurisdiction of a state court in case of a dispute. This is unfortunate as even if on-chain actors cannot be identified in the physical world, it is possible to determine the crypto assets stored in their wallet, such as cryptocurrencies, governance tokens of a DAO, or Non-Fungible Tokens (NFTs), which are assets that could potentially be used as compensation for the damage suffered by the DAO in its contractual relationship.

Off-chain actors are third parties acting on the blockchain who can be identified in the physical environment, for example through a KYC procedure. As they can be identified, the courts of their state of domicile or habitual residence may have personal jurisdiction over them in case of a dispute. If that state recognises the DAO's right to sue in its own name, the DAO, having suffered economic damage, could initiate proceedings against the off-chain actor to obtain reparation. In case of a regulated DAO, if the forum is not in its state of incorporation, the DAO's capacity to sue in its own name depends on its legal status in the state where the legal proceedings are initiated. It can be assumed that the regulated DAO would be granted the right to sue and be sued on the same basis as other foreign companies. The situation is much more uncertain in case of a maverick DAO, as no law grants those DAOs the right to be parties to proceedings in their own name. This puts members of maverick DAOs at a substantial disadvantage with regard to regulated DAOs in case of a dispute of a contractual nature.

3.3.3 Location of the Performance of the Contract

The forum at the place of performance of the contract may offer an interesting alternative to the forum of the defendant's domicile or seat. In order to determine the place of performance of the contract, the characteristic performance of the contract must usually be identified and located. Such is the case, for example, in Switzerland (Article 113 of the PILA). Under Swiss PIL, in contracts for the transfer of property, the characteristic performance is the transferor's

111 See *e.g.*, Art. 112 para. 1 of the PILA or Art. 2 para. 1 of the Lugano Convention.

112 See Kaal and Calcaterra (n 82), 133, who are of the opinion that it is impossible to locate the parties to a smart contract transaction.

obligation; in contracts to perform services (such as a mandate or a contract for work and services),[113] it is the service obligation; and in guarantee or suretyship agreements, it is the obligation of the guarantor or surety (Article 117 para. 3 of the PILA). Determining the characteristic performance can be difficult for certain types of contracts,[114] such as swap contracts. Even though Article 113 of the PILA does not specifically consider this alternative,[115] falling back on the principle of the closest connection could possibly offer an adequate solution to admit the jurisdiction of Swiss courts when no characteristic performance can be identified.[116] However, locating the performance of the contract in the process of finding a forum is not done the same way in all jurisdictions. Some PIL rules determine the place of performance by referring to the place where the contentious performance must be executed,[117] thus granting the courts of that state jurisdiction over the dispute. In any case, locating the performance of the contract can be difficult when it is performed on the Internet even when considering the principle of the closest connection.[118] And with smart contracts, locating the performance of the contract in a state jurisdiction becomes virtually impossible as the performance takes place exclusively on the blockchain.[119]

To illustrate the impossibility to locate smart contracts in a state jurisdiction, let's take as an example a smart contract between a DAO and a third party that stipulates that if the course of the ether reaches USD 3,500, the DAO must transfer one ether to the third party who in turn must transfer 15,000 dogecoins to the DAO. Under Swiss law, this kind of smart contract would qualify as a swap contract and can only be located with the principle of the closest

113 A contract for work and services (in French *contrat d'entreprise*) should not be confused with an employment contract. Under Swiss law, a contract for work and services (Art. 363 ff CO) is deemed to be concluded between parties of equal power, whereas an employment contract (Art. 319 ff CO) is deemed to be concluded between a stronger party (the employer) and a weaker party (the employee). Swiss PIL provides for specific connecting criteria for contracts with a weaker party such as an employment contract (Art. 115 of the PILA).

114 Andrea Bonomi, "Article 113 PILA," in Andreas Bucher (ed), *Commentaire romand. Loi sur le droit international privé – Convention de Lugano* (Helbing Lichtenhahn 2011), para. 16.

115 See Bonomi (n 114), para. 16.

116 However, this solution would be in contradiction with the jurisprudence of the Swiss Supreme Court (ATF 145 III 190). In Swiss PIL, the connection to the state with closest connections is indeed a fall-back rule in matters of applicable law (Art. 117 para. 1 of the PILA), but not in matters of jurisdiction (Art. 113 of the PILA).

117 See *e.g.,* Art. 5 para. 1 of the Lugano Convention. The jurisdiction of Swiss courts must be based on this provision when the defendant is domiciled in another contracting state to the Lugano Convention.

118 Bonomi (n 114), para. 28.

119 Guillaume (n 106), 56.

connection since it has no characteristic performance. As the smart contract is on the blockchain, and the object of the contract deals with the swap of cryptocurrencies which are on the blockchain, it can be concluded that the smart contract has its closest connection with the blockchain and not with a state jurisdiction. It must be concluded that there is no forum at the place of performance of such a smart contract in Switzerland, even if Article 113 of the PILA is interpreted in a broad sense that would grant jurisdiction to Swiss courts when the smart contract has its closest connection with that state.

Let's take as another example the case where a DAO publishes a smart contract calling for the development of an Information Technology (IT) solution by a software engineer. According to the offer, payment is done monthly in ethers until full accomplishment of the IT solution, and each payment is subjected to the achievement of determined monthly goals. We will assume that this smart contract amounts to a contract for work and services with payment instalments.[120] The development of the IT solution would be considered as the characteristic performance of this smart contract, and the performance of the contract would thus be located at the place where the IT solution is being developed. If this place is in Switzerland, Swiss courts would have jurisdiction in case of a dispute (Article 113 of the PILA). However, as the development and delivery of the IT solution happen both online, locating the performance of the contract in a state jurisdiction could prove difficult, and even irrelevant in many instances. The fall-back solution could be to locate the contract at the usual place of work of the engineer, where the computer is connected to the Internet.[121] However, while this forum exists in Swiss PIL for employment contracts,[122] it is not provided for in the case of contracts for work and services. Furthermore, the software engineer taking the offer could be a digital nomad who works from many different places, making any connection to a particular state jurisdiction irrelevant. Even more so if the software engineer

120 The characterisation of the contract depends on the law governing the contract. It is not uncommon for courts to reconsider the characterisation intended by the parties by recharacterising certain contractual relationships. For example, a contract for work and services (n 113) could be recharacterised as an employment contract when there is a relationship of economic dependence between the parties. See Florence Guillaume, "Le contrat de travail international: règles de droit international privé et plateformes numériques," in Jean-Philippe Dunand and Pascal Mahon (eds), *Les aspects internationaux du droit du travail* (Schulthess 2019), 193, 234.

121 See Guillaume (n 120), 240.

122 The Swiss courts of the place where the employee habitually performs their work have jurisdiction over an employment contract (Art. 115 para. 1 of the PILA). The same rule can be found in the Lugano Convention (Art. 19 para. 2).

is pseudonymous, in which case no connection to a state jurisdiction is possible. Here again, the closest connection of the contract is with the blockchain, as the smart contract itself is deployed on the blockchain, the work is done online, and the payment is executed on the blockchain with a cryptocurrency. The forum at the place of performance of the smart contract is therefore of no use in this case.

Even if objective connecting factors of PIL fail to connect smart contracts to a state jurisdiction, parties who want to address the risk of not having their contractual relationship linked to a state jurisdiction can agree in the smart contract on the place of performance. Indeed, party autonomy allows them to create a subjective link with a state jurisdiction. By determining the place of performance in the smart contract, the parties can influence the jurisdiction of the state courts. Depending on the rules of PIL of the chosen state, the courts of that state could have jurisdiction over disputes in contractual matters. For example, the courts of the contracting states of the Lugano Convention will admit their jurisdiction for disputes in contractual matters when the parties have fixed, in their contract, the place of performance of the obligation in question in their state.[123] An agreement of the parties on the place of performance of the contractual obligations can thus have an effect on the jurisdiction of the state courts. In this way, the parties to the smart contract can create a connection with a jurisdiction that grants smart contracts a legal scope, which offers them a certain degree of legal certainty in case of a dispute. But other legal challenges could still prevent any of the parties from initiating legal proceedings in case of non-execution or improper execution of the contract, such as the DAO not having the capacity to sue or be sued in its own name in the chosen jurisdiction, or the impossibility to identify the other party because of its pseudonymity. In any case, it would not make sense for the parties to a smart contract to choose Switzerland as the place of performance of the contract because the legal scope of smart contracts and DAOs is still uncertain in that state.

3.4 *Universal Jurisdiction as an Alternative to Connecting Factors*

As we have seen above,[124] connecting factors of PIL fail to connect legal situations involving a DAO in many different instances, whether we try to locate the DAO, a member of the DAO, the smart contract, or a third contracting party.

123 Art. 5 para. 1 of the Lugano Convention. See Andrea Bonomi, "Article 5 LC," in Andreas Bucher (ed), *Commentaire romand. Loi sur le droit international privé – Convention de Lugano* (Helbing Lichtenhahn 2011), para. 64.

124 See *supra* chapters 3.2 and 3.3.

Pseudonymity within the blockchain environment usually prevents the localisation of individuals (DAO members or third contracting parties), smart contracts are executed exclusively on the blockchain, and maverick DAOs have no connection to state jurisdictions. Some reliable connections to a state jurisdiction could nevertheless be identified but they only work in specific cases: when the DAO has a seat, when it has a registered representative, or when the DAO has a contractual relationship with an off-chain actor. As this is not the case in the vast majority of legal situations involving a DAO, PIL rules usually lead to a dead-end. The lack of access to justice results in a situation of great legal uncertainty for DAOs, their members and the third contracting parties.

When no state can provide an effective forum, there is no alternative but to consider that state courts should exercise universal jurisdiction. Some states establish in their law a forum of necessity when no other state offers the jurisdiction of its courts, on the condition that there is a sufficient connection with the state of the forum.[125] Universal jurisdiction goes further in that the jurisdiction does not necessarily require the existence of geographical links with the state of the forum. It is worth briefly discussing the merits of introducing universal jurisdiction for disputes involving DAOs.

Universal jurisdiction does not attribute jurisdiction to a particular state but allows the courts of any state to admit their jurisdiction. It has a global scope that is appropriate for legal relationships that are global in scope and therefore do not have close connections with a particular state. Not only does a relationship involving a DAO require the use of the Internet, which is a tool whose scope is both universal and ubiquitous,[126] but the existence of both the DAO and its contractual obligations are materialised on the blockchain, which is a distributed global network of nodes.[127] Given the difficulty, if not the impossibility, of connecting legal situations involving a DAO to a state by means of objective connecting criteria, it might be appropriate to consider that this type of relationship has an intrinsically global scope when discussing the issue of dispute resolution. Admitting universal jurisdiction would allow for the bringing of a dispute involving a DAO to the courts of any state for resolution. Jurisdiction should, however, be exercised only if the *ratione materiae*,

125 *E.g.*, in Switzerland, Art. 3 of the PILA: "When this Act does not provide for jurisdiction in Switzerland and proceedings in a foreign country are impossible or cannot reasonably be required, the Swiss judicial or administrative authorities at the place with which the case has sufficient connection have jurisdiction."

126 Guillaume (n 1), 174–175.

127 Florence Guillaume, "Aspects of Private International Law Related to Blockchain Transactions," in Daniel Kraus, Thierry Obrist and Olivier Hari (eds), *Blockchains, Smart Contracts, Decentralised Autonomous Organizations and the Law* (Edward Elgar 2019), 49, 59–60.

personae and *loci* components of jurisdiction converge to some extent, in the particular case, on the court in question, since it must be able to settle the dispute effectively and fairly.[128]

The fact remains that universal jurisdiction allows the plaintiff, to a large degree, to choose freely before which state court to bring legal proceedings according to its own interests. Forum shopping causes legal uncertainty for the defendant who may be sued before any court and may be subject to any law. There is (almost) no means to know in advance where a lawsuit could be filed. In this way, the plaintiff is favoured, being in a position to choose the forum and indirectly the law applicable to the claim, to the detriment of the defendant.[129] In practice, it is very likely that the plaintiff would choose to act before the courts of the state in which they are domiciled, which would give the plaintiff a clear advantage in the proceedings. This puts DAOs and any person involved with them at risk of being sued anywhere and to be subject to any law. This situation is problematic given the legal uncertainty related to the legal status of DAOs.

The admission, from a theoretical point of view, that a dispute involving a DAO may be submitted to the courts of any state by recognising the existence of universal jurisdiction does not mean that, in practice, the courts of any state will accept their jurisdiction and rule on the dispute. In the absence of an obligation resulting from an international convention, each state is free to decide the circumstances in which its courts have jurisdiction over a dispute which is international in scope. A state will only grant the protection of its courts if it considers having an interest in offering the plaintiff the possibility of obtaining compensation on its territory. A state's interest in offering the protection of its courts to a legal relationship that is carried out and validated only in the digital space of the blockchain is not obvious.

In disputes involving DAOs, universal jurisdiction would allow any DAO, DAO member, and third contracting party to initiate proceedings in the courts of their choice. This way, they are guaranteed access to justice. However, this does not address the issue of the legal capacity of maverick DAOs, nor the issue of the pseudonymity of the blockchain environment. In practice, the scope of the universal jurisdiction would be considerably reduced. Firstly, it would be possible to seize a court only in the states that recognise legal capacity for DAOs. Otherwise, the DAO would not have the capacity to sue or be sued in its

128 Andreas Bucher, "La compétence universelle civile en matière de réparation pour crimes internationaux" (2015) 76 Annuaire de l'Institut de droit international 1, 89–90.

129 The applicable law is frequently an incentive for the choice of the forum. See *e.g.*, Svantesson (n 104), 487–488.

own name in the state of the forum. Secondly, the legal proceedings could not be initiated if the defendant cannot be identified. Therefore, admitting universal jurisdiction does not guarantee that a dispute involving a DAO can be decided by a state court.

3.5 *Enforcement of a Court Decision on the Blockchain*

Challenges to seeking justice in case of a dispute involving DAOs do not end with finding a court with jurisdiction over the dispute. Even if a state court has jurisdiction and issues a decision, the aggrieved party may find it impossible to seek the enforcement of the decision on the blockchain when the losing party does not spontaneously comply.

Traditionally, the guarantee of enforcement of a court decision has been established by coercive force exerted by the states which maintain a monopoly over the use of force on their territory.[130] However, states have limited enforcement power: they have no right to enforce the decisions rendered by their courts abroad. When it comes to executing a decision on the blockchain, it is not the law, but the technology that prevents states from exercising their power of enforcement. The immutability that characterises blockchain technology does not allow any authority to modify the content of the blockchain. Hence, state authorities have no enforcement power over assets in the crypto space as blockchain technology is tamper-proof.

For instance, enforcement of court decisions related to the governance of a DAO is problematic. The rules dictating the governance of a DAO are inscribed on immutable smart contracts spread on a global network of computers. This results in censorship resistant entities that are created and exist autonomously from any central authority. Only the community of members acting within the parameters of the code can trigger an action from the entity. Crypto assets share the same immutable characteristics. One member does not have the power to dispose of the DAO's crypto assets if the code does not allow for it. No enforcement authority can force an action upon the DAO and the DAO's crypto assets cannot be frozen, seized, or confiscated. Therefore, no coercive measure can be enforced on a DAO. The DAO project outlined the risks of using DAOs and showed that by relying on a peer-to-peer decentralised infrastructure, DAOs

130 Pietro Ortolani, "The Judicialization of the Blockchain," in Philipp Hacker and others (eds), *Regulating Blockchain – Techno-Social and Legal Challenges* (2019 Oxford University Press), 289, 303, states that "[w]hile private parties are left free to opt out of state court litigation by submitting to arbitration, they are always required to apply for state-controlled enforcement procedures whenever they need to obtain the coercive execution of the final outcome."

fall outside the reach of state jurisdictions.[131] And with the pseudonymity that DAO members enjoy on the blockchain, enforcement authorities cannot force them to execute an action, on the blockchain or outside the blockchain. State authorities are left with no enforcement power, either on the organisation, its assets, or its members, at least for maverick DAOs.

The problem of enforcement of state court decisions is similar in the case of a decision concerning a contractual relationship between a DAO and a third party formalised by means of a smart contract. Since smart contracts are immutable,[132] state authorities cannot exercise their enforcement power to adapt the execution of smart contracts, to stop them from executing all together, or to restore the initial situation if smart contracts have been improperly executed. For instance, if a state court orders the creation of a new smart contract to cancel the effects of the one that has been improperly executed, which is referred to as a "reverse transaction," such a decision cannot be enforced by force using state enforcement authorities. According to some authors, "[c]ourts cannot require a retroactive change in the blockchain because that is computationally near impossible."[133] This would go against the immutability of the blockchain.[134] As no one has the power to update the code of smart contracts once they are launched on the blockchain,[135] state enforcement authorities have no means to stop the execution or to freeze the crypto assets held by a particular smart contract, even if that smart contract falls within their jurisdiction. Such power could only belong to the community of a blockchain. The DAO case showed that in extreme situations the community can make the decision to change the status of the ledger.[136] However, it is highly unlikely that

131 See *supra* chapter 2.1.

132 See *supra* chapter 3.1.

133 Kaal and Calcaterra (n 82), 137. See also Werbach and Cornell (n 83), 331–333.

134 However, De Filippi and Wright (n 13), 208, noted that states could "exert pressure on the intermediaries in charge of developing, deploying, or maintaining the technology" and "[i]n the case of harm, they could demand that miners censor certain transactions or even revert the blockchain back to its previous state to recover damages or remedy harm." If a state cannot directly enforce its decisions on a blockchain, it can indeed enforce them indirectly through individuals or companies that have influence over its operation and are located in its territory.

135 According to Christoph Müller, "Les 'smart contracts' en droit des obligations suisse" in Blaise Carron and Christoph Müller (eds), *3e Journée des droits de la consommation et de la distribution, Blockchain et Smart Contracts – Défis juridiques* (Helbing Lichtenhahn 2018), para. 93, the fact that the execution of smart contracts cannot be stopped or modified raises a number of legal issues. See also Sarah Templin, "Blocked-Chain: The Application of the Unauthorized Practice of Law to Smart Contracts" (2019) 32 The Georgetown Journal of Legal Ethics 957, 961.

136 See *supra* chapter 2.1.

such a decision would be made to enforce a court decision on a mere contractual relationship involving a DAO.

The inability of states to exercise their enforcement power on the blockchain means that the enforcement of court decisions on the blockchain relies exclusively on the willingness of the parties. This leads to a significant risk of non-compliance with the decision of a state court because people know that coercive enforcement is not a realistic possibility.[137] Since states have no power to enforce court decisions on the blockchain, the efficiency of justice cannot be guaranteed. This observation has led some authors to say that "enforcement [on the blockchain] could be a lost cause."[138]

3.6 *Need for an Alternative to State Courts for Disputes Involving DAOs*

The discussion above has shown that it is a challenge to offer the protection of state courts in a reliable way when the legal situation involves the use of blockchain technology. The uncertainties around the jurisdiction of state courts for disputes involving DAOs are not desirable. We have seen that most of the times state courts do not have jurisdiction over disputes involving DAOs as it is not possible to establish sufficient connections outside of the blockchain environment. It is of course possible to remedy this legal uncertainty by making a choice of court. For example, the parties to a smart contract could insert a choice of court clause in the code of the smart contract and thus agree to submit a possible dispute to the courts of a specific state. A choice of court agreement would mainly serve at providing a forum for disputes involving a maverick DAO or an on-chain actor as they cannot be linked to a state jurisdiction with objective connecting criteria and no court has personal jurisdiction over them. But this option is purely theoretical as no state recognises the legal scope of maverick DAOs,[139] and on-chain actors are pseudonymous.[140] As a result, even if a link with a state does exist, the courts that have jurisdiction may not be able to effectively administer justice. This may hinder the aggrieved party from seeking compensation for the damage. As a result, on top of an important legal uncertainty, there is a great risk of denial of justice in disputes involving DAOs.

---

137 See Henry H. Perritt, "Towards a Hybrid Regulatory Scheme for the Internet" (2001) University of Chicago Legal Forum 215, 258. However, it is true that the court decision could order a compensation (*e.g.*, the payment of damages) to circumvent the impossibility of being executed on the blockchain. See also Clément (n 86), 285–286.

138 Rabinovich-Einy and Katsh (n 86), 73.

139 See *supra* chapter 2.3.1.

140 See *supra* chapter 3.3.2.

This unsatisfactory situation calls for the search for alternatives to state justice for disputes involving DAOs. This leads us not to ask where to take legal action, but what is the most appropriate dispute resolution mechanism to settle this kind of disputes: one that takes advantage of blockchain technology and smart contracts. Indeed, actors of the blockchain environment have crypto assets stored in their wallets, such as cryptocurrencies, DAO governance tokens, or NFTs, and new dispute resolution mechanisms could be developed to take advantage of this situation by enforcing their decisions on those crypto assets.

These alternatives to state justice could take into account the immutability of the blockchain to set up means to have decisions enforced that do not require the exercise of coercive power. For example, damage to reputation may be decisive for voluntarily compliance with a decision. In relation to the famous Yahoo! case,[141] it was noted that "even in the absence of enforceability, factors such as market forces or moral beliefs, or a combination of them, may by themselves or in combination with legal measures compel legal compliance."[142] DAOs that want to have a lasting activity in the crypto environment must maintain a certain reputation. This is key to attracting investments and expanding activities. It can therefore be assumed that DAOs have an important incentive to spontaneously enforce a decision on a dispute involving them in order to preserve their reputation. One notorious example is The DAO case: the risk of damage to the reputation of the blockchain Ethereum proved to be a sufficient incentive to restore a state of justice even in the absence of a formal court decision.[143] But the threat of damage to the reputation could only work against entities that need to maintain a good reputation. For a DAO with no reputation and whose members are hidden behind their pseudonymity, voluntary enforcement might be unattainable.

4 Lessons Learned from Online Dispute Resolution (ODR)

The difficulty to connect a legal situation to a state has already been a challenge in the field of international commercial relations, which is one of the reasons

141 Tribunal de Grande Instance de Paris, 20 November 2000, *LICRA and UEJF v. Yahoo! Inc. and Yahoo! France*, and U.S. Court of Appeals for the Ninth Circuit, 24 November 2005, *Yahoo! Inc. v. LICRA and UEJF*, 433 F.3d 1199 (9th Cir. 2006).

142 Uta Kohl, *Jurisdiction and the Internet. Regulatory Competence over Online Activity* (Cambridge University Press 2007), 207.

143 See *supra* chapter 2.1.

that led to the search for alternatives to state justice. Among the Alternative Dispute Resolution (ADR) mechanisms (ADRs)[144] offered by private justice, arbitration has long been the preferred option in cross-border business relationships (4.1). The advent of e-commerce has led to the development of other types of simpler, faster and cheaper dispute resolution models to absorb the huge number of small claim disputes. The implementation of Online Dispute Resolution (ODR) mechanisms (ODRs) helped to circumvent the issue of jurisdiction and applicable law in online transactions. This has resulted in the creation of a private justice system parallel to the state justice system which is, to a large extent, beyond the influence of national laws (4.2).

The pathway towards private justice seems just as relevant for disputes involving DAOs than for other types of online transactions. It is worth taking a brief look at the ADRs that have been put in place for online transactions, and in particular for e-commerce, because the experience gained with those private justice systems is the basis for the development of new ODRs for disputes involving DAOs.

4.1 *Alternative Dispute Resolution in the Form of Arbitration*

The most common form of ADR used to resolve disputes regarding international commercial relations is arbitration. Parties to a legal relationship decide, in an arbitration agreement, that, in case of a dispute, a third independent person will act as a judge and resolve a conflict by issuing a decision. A distinction must be made between classic arbitration where the decision rendered is equal to a court judgment (4.1.1) and other forms of ADRs which also make use of the services of a neutral third party to render a decision for the parties but whose decisions cannot be considered as equal to court judgments (4.1.2).

4.1.1 Classic Arbitration

Arbitration has the main advantage of rendering decisions that are not only binding on the parties but also have a scope equivalent to that of a judicial decision when the procedure followed by the arbitrators is established or recognised by the states. Arbitral awards have in principle a *res judicata* effect and are considered as such equal to judgments rendered by state courts. The exact legal scope of an arbitral award depends on the law of the state in which it is rendered. It is the national law that confers enforceability and the *res judicata*

144 About ADRs, see *e.g.*, Michael Palmer and Simon Roberts, *Dispute Processes – ADR and the Primary Forms of Decision-making* (3rd edn, Cambridge University Press 2020).

effect on the arbitral award.[145] In some states, the arbitral award has a *res judicata* effect as soon as it is rendered, in others, as soon as it is notified to the parties, and in others, as soon as it is declared enforceable following recognition and enforcement proceedings.[146] In Switzerland, for example, an arbitral award has "the effect of a legally-binding and enforceable judicial decision" as soon as "notice of the award has been given to the parties."[147] This means that the award is enforceable and acquires a *res judicata* effect from its notification to the parties. The arbitral award can thus be enforced immediately in Switzerland.[148]

Arbitration is in principle linked to a state by the seat of arbitration.[149] An arbitration whose seat is in Switzerland renders a Swiss arbitral award. Being final, a Swiss arbitral award is enforceable by Swiss authorities in the same manner as a judgment rendered by a Swiss court.[150] The seat of arbitration is in principle designated by the parties or the arbitration institution chosen by them. It may also be determined by the arbitrators themselves, in particular in the case of *ad hoc* arbitration.[151]

Arbitral awards not only have effect in the state of the seat of arbitration but may also have legal effect in other states. However, enforcement of an arbitral award in a state other than the one in which it was rendered is usually possible only if the award is enforceable in the state of the seat of arbitration. Additionally, the conditions for recognition and enforcement provided for in the rules of PIL of the state where enforcement is requested (the "requested state") must also be fulfilled, just like the recognition and enforcement of foreign judgments.

145 See *e.g.*, Gabrielle Kaufmann-Kohler and Antonio Rigozzi, *International Arbitration – Law and practice in Switzerland* (Oxford Academic 2015), para. 1.18.

146 See *e.g.*, Mauro Rubino-Sammartano, *Arbitrage international*, vol. 2 (Bruylant 2019), para. 28.275–28.295; Jean-François Poudret and Sébastien Besson, *Comparative Law of International Arbitration* (2nd edn, Sweet & Maxwell 2007), para. 475.

147 See Art. 387 Swiss Civil Procedure Code (SR 272). The same rule applies when the arbitration is international (Art. 190 para. 1 of the PILA).

148 See *e.g.*, Kaufmann-Kohler and Rigozzi (n 145), para. 7.187; Bernhard Berger and Franz Kellerhals, *International and Domestic Arbitration in Switzerland* (3rd edn, Stämpfli 2015), para. 1633–1636, and para. 2006–2026.

149 See *e.g.*, Berger and Kellerhals (n 148), para. 743; Poudret and Besson (n 146), para. 134–135.

150 See *e.g.*, Kaufmann-Kohler and Rigozzi (n 145), para. 1.18; Berger and Kellerhals (n 148), para. 1629.

151 See *e.g.*, Kaufmann-Kohler and Rigozzi (n 145), para. 2.17–2.22; Berger and Kellerhals (n 148), para. 746–766.

The Convention on the Recognition and Enforcement of Foreign Arbitral Awards of 10 June 1958 (the "New York Convention")[152] is applicable if enforcement is sought in a contracting state. In this case, the New York Convention provides a set of harmonised rules for the recognition and enforcement of arbitral awards, facilitating this process. The recognition and enforcement of an arbitral award are only granted under this convention if fundamental procedural rights of the parties have been respected in the procedure leading to the arbitral award. The scope of the awards that fall under the New York Convention is not precise and raises questions of interpretation. They are defined as "not only awards made by arbitrators appointed for each case but also those made by permanent arbitral bodies to which the parties have submitted."[153] An arbitral award may be recognised and enforced as soon as it has become "binding on the parties."[154] Legal scholars consider that the New York Convention is in principle only likely to apply to awards which definitively establish the rights and obligations of the parties and whose solution on the merits cannot be called into question at a later trial.[155] This allows an arbitral award that falls within the scope of the New York Convention to be easily enforced in the numerous countries that are parties to the Convention if the losing party does not voluntarily enforce the award.

4.1.2 Non-binding Arbitration

Some forms of ADR are often referred to as "arbitration," even though they fundamentally differ from arbitration in that the outcome is usually not enforceable by state authorities and does not have a *res judicata* effect. The reason is that while those ADRs offer a decision rendered by a third party, in the same way as arbitration, the procedure is not governed by the rules of arbitration and is less stringent. Compared to arbitration, they are deemed to have the advantage of offering a faster and more cost-effective way to resolving disputes. But fundamental procedural rights of the parties are not necessarily respected. We will hereafter refer to those ADRs, which are binding on the parties as a contractual obligation but do not produce decisions equal to

152 SR 0.277.12.

153 Art. 1 para. 2 of the New York Convention.

154 Art. V para. 1 sub-para. e of the New York Convention.

155 Andreas Bucher, "Article 194 PILA," in Andreas Bucher (ed), *Commentaire romand. Loi sur le droit international privé – Convention de Lugano* (Helbing Lichtenhahn 2011), para. 20. See also *e.g.*, Kaufmann-Kohler and Rigozzi (n 145), para. 8.240–8.244.

judgments rendered by state courts, as "non-binding arbitration"[156] to distinguish them from classic arbitration.[157]

Decisions made in the context of non-binding arbitration proceedings do not have the effect of legally binding and enforceable judicial decisions. They are not enforceable by state authorities in the same manner as judgments rendered by state courts, nor do they fall within the scope of the New York Convention. The execution of the outcome of non-binding arbitration depends entirely on the willingness of the losing party. However, the non-execution of the decision would equate to the non-execution of a contractual obligation. In the absence of voluntary compliance, the decision can thus be enforced by state authorities if the party seeking execution obtains a judgment which orders the other party to execute the performance due. When it comes to an international business relationship, questions of PIL resurface at the time of the "enforcement" of the outcome of non-binding arbitration and complicate the judicial procedure. To obtain a court decision ordering the execution of the performance due, it is indeed necessary to determine the forum and the applicable law. This generates disproportionate costs that are likely to discourage the successful party from seeking a judicial decision. There is thus a significant risk that the decision is not spontaneously executed by the losing party who is well aware of the difficulties related to the execution of the outcome of non-binding arbitration with the assistance of state authorities.

However, the losing party may be willing to execute the outcome of non-binding arbitration when it considers that the decision was rendered by a truly impartial expert in fair proceedings in which fundamental procedural rights, including the right to be heard, have been respected.[158] If the execution of the decision is done spontaneously, it is not necessary to rely on the assistance of state authorities to obtain satisfaction. In this case, the settlement of the dispute by non-binding arbitration has the advantage of circumventing the delicate issues of PIL, while obtaining a resolution of the dispute in a simple way.

156 This term was introduced by Thomas Schultz, "Online Arbitration: Binding or Non-Binding?" (*ADROnline Monthly*, November 2002), 3.

157 About non-binding arbitration, see also Thomas J. Stipanowich, "The Arbitration Penumbra: Arbitration Law and the Rapidly Changing Landscape of Dispute Resolution" (2007) 8 Nevada Law Journal 427, 448–455; Steven C. Bennett, "Non-binding Arbitration: An Introduction" (2006) 61 Dispute Resolution Journal 1; Gabrielle Kaufmann-Kohler and Thomas Schultz, *Online Dispute Resolution – Challenges for Contemporary Justice* (Kluwer Law International 2004), 153–168.

158 Schultz (n 156), 8.

4.2 *ODR in the Field of E-commerce*

ADR is commonly used in the field of e-commerce, where it provides a good substitute for state justice. Legal proceedings in state courts very often appear inadequate because they are too complex and costly in view of the value in dispute. Understandably, e-commerce platforms have carried out an online migration of ADR by developing ODR (4.2.1). As ODRs which use arbitration are usually non-binding arbitration proceedings, the effectiveness of the decisions rendered by ODR in e-commerce matters relies essentially on the voluntary compliance by the losing party (4.2.2).

4.2.1 Bringing Alternative Dispute Resolution Online

The international character of e-commerce transactions leads to complicated court proceedings with difficult PIL issues regarding the localisation of the legal relationship.[159] The legal situation of the parties to an e-commerce relationship is all the more complicated as there is no international instrument of worldwide scope that establishes rules of jurisdiction in the field of e-commerce. Until now, states have concentrated their efforts to harmonise the law on rules of substantive law without intervening in the jurisdiction of their courts to judge e-commerce disputes. The huge number of disputes could not, in any case, be absorbed by state courts. There is thus a risk that consumers find themselves not only in situations of significant legal uncertainty, but also unable to assert their rights in court. This is why the implementation of ADR has become the only way to resolve the exponential increase of cross-border small-claim disputes generated by this new mode of consumption.[160] Setting up ADRs conducted online quickly emerged as the best solution to provide an efficient, cost-effective, and flexible way to resolve disputes arising from e-commerce.[161]

E-commerce platforms recognised the link between the growing adoption of e-commerce and the resolution of e-commerce disputes. They see ODR as a key measure to attract new customers since providing a conflict resolution mechanism which is adapted to the needs of users reduces the risks of

159 See *e.g.*, Colin Rule, Vikki Rogers and Louis F. Del Duca, "Designing a Global Consumer Online Dispute Resolution (ODR) System for Cross-Border Small Value - High Volume Claims – OAS Developments" (2010) 42 Uniform Commercial Code Law Journal 221, 225–228.

160 See Ethan Katsh and Orna Rabinovich-Einy, *Digital Justice – Technology and the Internet of Disputes* (Oxford University Press 2017), 4–13.

161 See Faye Fangfei Wang, *Internet Jurisdiction and Choice of Law – Legal Practices in the EU, US and China* (Cambridge University Press 2010), 143–144; Palmer and Roberts (n 144), 290–291.

contracting online and generates a higher level of trust in the system.[162] In the words of Pablo Cortés, "the goal of ODR is not just to settle disputes but also to increase confidence in e-commerce"[163] and, thus, to stimulate trade.[164] By reducing the risk of denial of justice, ODR strengthens user trust in the business environment offered by the e-commerce platform.

Dispute resolution by means of classic arbitration conducted online is rarely considered for e-commerce disputes, as the law of several countries provides that disputes concerning consumer contracts cannot be settled by arbitration or only if specified conditions are met. This is the case, for example, in the European Union (EU), where the system of protection of consumers is based on "the idea [...] that the consumer is in a weaker position vis-à-vis the seller or supplier, as regards both his bargaining power and his level of knowledge, which leads to the consumer agreeing to terms drawn up in advance by the seller or supplier without being able to influence the content of those terms."[165] It follows that an arbitration agreement is viewed as unfair if it has not been "individually negotiated" and "causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer," "contrary to the requirement of good faith."[166] Unfair pre-dispute

---

162 See Faye Fangfei Wang, *Online Arbitration* (Routledge 2018), 6–7; Katsh and Rabinovich-Einy (n 160), 10; Thomas Schultz, "Does Online Dispute Resolution Need Governmental Intervention? The Case for Architectures of Control and Trust" (2004) 6 North Carolina Journal of Law & Technology, 71, 105; Colin Rule, "Quantifying the Economic Benefits of Effective Redress: Large E-Commerce Data Sets and the Cost-Benefit Case for Investing In Dispute Resolution" (2012) 34 University of Arkansas at Little Rock Law Review 767, 774–776.

163 Pablo Cortés, "Online Dispute Resolution for Consumers – Online Dispute Resolution Methods for Settling Business to Consumer Conflicts," in Mohamed S. Abdel Wahab, Ethan Katsh and Daniel Rainey (eds), *Online Dispute Resolution: Theory and Practice* (eleven 2012), 139, 150.

164 Pablo Cortés, "The New Landscape of Consumer Redress," in Pablo Cortés (ed), *The New Regulatory Framework for Consumer Dispute Resolution* (Oxford University Press 2016), 17, 35.

165 ECJ, 17.05.2018, C-147/16, *Karel de Grote – Hogeschool Katholieke Hogeschool Antwerpen vzw v. Susan Romy Jozef Kuljpers*, ECLI:EU:C:2018:320, para. 54.

166 Art. 3 para. 1 of the Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts ([1993] OJ L 95/29). It should be noted that Directive 93/13/EEC has been amended twice. First, by Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council ([2011] OJ L 304/64). Second, by Directive (EU) 2019/2161 of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council as regards the better enforcement and

arbitration agreements in consumer contracts are not binding on consumers.[167] The same rule applies to pre-dispute ODR agreements, in particular where they are contained in contracts whose terms have not been individually negotiated.[168] The validity of pre-dispute arbitration agreements in the field of e-commerce and their effect on consumers raise significant difficulties in practice. As a result, states are unable to find a harmonised solution on this issue.[169] If we also consider that classic arbitration is often too expensive for small-claim disputes, this explains the reason why ODRs that are aimed at e-commerce disputes usually take the form of non-binding arbitration.

Therefore, when e-commerce platforms want to offer their users an ODR mechanism whereby they can obtain a decision rendered by a third party, they usually use non-binding arbitration. As the outcome of non-binding arbitration does not have the effect of a legally binding and enforceable judicial decision, and thus does not acquire *res judicata* effect, e-commerce platforms that subject their users to this type of ODR can guarantee a simple, fast, and

---

modernisation of Union consumer protection rules ([2019] OJ L 328/7), which requires that EU countries introduce effective, proportionate and dissuasive sanctions to punish businesses that breach the rules on unfair contract terms. Directive (EU) 2019/2161 must be transposed into the national legislation of the EU countries before 28 November 2021.

167 See Art. 6 of the Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts ([1993] OJ L 95/29), which provides that "unfair terms used in a contract concluded with a consumer […] [shall] not be binding on the consumer."

168 European Commission, Guidance on the interpretation and application of Council Directive 93/13/EEC on unfair terms in consumer contracts (2019/C 323/04), [2019] OJ C 323/4, 62. See also recital 43 of the Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) N 2006/2004 and Directive 2009/22/EC (Directive on Consumer ADR), [2013] OJ L 165/63, which states that "[a]n agreement between a consumer and a trader to submit complaints to an ADR entity should not be binding on the consumer if it was concluded before the dispute has materialized and if it has the effect of depriving the consumer of his right to bring an action before the courts for the settlement of the dispute."

169 The fact that UNCITRAL had to give up adopting Rules on ODR providing rules and guidelines in the field of ODR for e-commerce transactions, including consumer contracts, is revealing in this respect. See UNCITRAL, "Report of Working Group III (Online Dispute Resolution) on the work of its twenty-sixth session (Vienna, 5–9 November 2012)," 19 November 2018, A/CN.9/762. Regarding the procedure which eventually led to the adoption of the Technical Notes, see *e.g.*, Riikka Koulu, *Law, Technology and Dispute Resolution – Privatisation of Coercion* (Routledge 2019), 125–129; Zbynek Loebl, *Designing Online Courts – The Future of Justice Is Open to All* (Wolters Kluwer 2019), 10–11; Pablo Cortés, "The Consumer Arbitration Conundrum – A Matter of Statutory Interpretation or Time for Reform?," in Pablo Cortés (ed), *The New Regulatory Framework for Consumer Dispute Resolution* (Oxford University Press 2016), 65, 73–75.

cost-efficient way to resolve disputes, while still allowing their users to resort to state courts for subsequent dispute resolution if they are not satisfied with the outcome of the non-binding procedure. If users were subject to classic arbitration, the *res judicata* effect of the arbitral award would prevent them from bringing an action before the courts for the settlement of the dispute, which would be contrary to many consumer protection laws.

4.2.2 Enforcement of an Online Arbitral Award

When an ODR mechanism provides classic arbitration conducted online and renders arbitral awards within the meaning of the New York Convention, recognition and enforcement of the arbitral award may be executed pursuant to that instrument. However, this situation rarely arises for decisions rendered by an ODR mechanism in e-commerce matters. Some contracting states of the New York Convention – such as the EU Member States – have expressly excluded arbitral awards in consumer disputes from the scope of application of the convention. In those states, it results from the law that a consumer cannot validly enter into an arbitration agreement, or only if certain conditions are met. The enforcement of an arbitral award against a consumer could therefore be problematic, or even impossible. In any case, the recognition and enforcement of the arbitral award could not benefit from the favourable regime established by the New York Convention.

In the field of e-commerce, in most cases where a decision is rendered online by a third party, the decision results from a non-binding arbitration procedure. As such, the decision is not enforceable by state authorities in the same manner as a judgment rendered by a state court, nor does it fall within the scope of the New York Convention.[170] The execution of the decision rests fundamentally on the willingness of the losing party, which raises an important issue. In this context of mass commercial relations based on one-shot transactions, which is specific to e-commerce, there is indeed a significant risk that the losing party does not comply spontaneously. This is a central issue because the possibility of obtaining execution by force is essential for the effective resolution of the dispute. This is not only a question of the proper functioning of the ODR mechanism, but also of confidence in the ability of the system to effectively resolve disputes.

In order to address the risk of non-compliance to the decision, e-commerce platforms seek to implement mechanisms that favour voluntary compliance with the outcome of the ODR proceedings. Those mechanisms are intended

170 See *supra* chapter 4.1.2.

to compensate for the fact that ODR platforms do not have the power to enforce the ODR outcome outside of their ecosystem and that it would be too complicated – and probably too expensive – to request the assistance of the state authorities to enforce the decision with traditional means. For example, the losing party may have incentives to abide by the decision when its market access or its reputation is at stake in the ecosystem in which the legal relationship between the parties is embedded.[171] Sellers risk losing customers if they are given poor ratings because they refuse to enforce decisions made by the ODR system of the e-commerce platform. Social and economic incentives, such as trustmarks, accreditation and reputation management systems, exclusion from the marketplace, blacklists, or even penalties for delay in performance,[172] have proved to be efficient incentives for voluntary compliance to non-enforceable decisions.[173] Such incentives are based not only on the willingness of the parties to comply with their agreement over the fact that decisions are binding, but also on the threat of a direct sanction on their property or rights, their ability to engage in business relations, their reputation, or even their belonging to a community (*i.e.*, an e-commerce platform). The power to deny access to a marketplace (*e.g.*, by banishing a user from an e-commerce platform) has not only a social impact, but also an economic impact. Voluntary compliance may therefore result from the pressure of the business and social environment. When the ODR platform controls the reputation of the users of the e-commerce platform, it may award or withdraw reputation points following the ODR outcome or based on voluntary compliance with the ODR outcome. Even though it is not a direct enforcement of the decision, the threat of ostracism puts social and economic pressure on community members to voluntary comply with decisions rendered in the course of an online non-binding arbitration procedure.

171 Colin Rule and Harpreet Singh, "ODR and Online Reputation Systems – Maintaining Trust and Accuracy Through Effective Redress," in Mohamed S. Abdel Wahab, Ethan Katsh and Daniel Rainey (eds), *Online Dispute Resolution: Theory and Practice* (eleven 2012), 163–184; Kaufmann-Kohler and Schultz (n 157), 225–227; Katsh and Rabinovich-Einy (n 160), 66.

172 See UNCITRAL, "Online dispute resolution for cross-border electronic commerce transactions: issues for consideration in the conception of a global ODR framework," 28 September 2011, A/CN.9/WG.III/WP.110, para 49.

173 See *e.g.*, Kaufmann-Kohler and Schultz (n 157), 228–233; Vikki Rogers, "Knitting the Security Blanket for New Market Opportunities – Establishing a Global Online Dispute Resolution System for Cross-Border Online Transactions for the Sale of Goods," in Mohamed S. Abdel Wahab, Ethan Katsh and Daniel Rainey (eds), *Online Dispute Resolution: Theory and Practice* (eleven 2012), 95, 102–104; Perritt (n 137), 237–240.

However, reputation management systems and mechanisms of control of access to the market are clearly insufficient on their own to generate users' trust in the business environment offered by an e-commerce platform.[174] Such tools favouring voluntary compliance with the ODR outcome appeared to be insufficient to build an architecture of confidence, that is to say "an architecture that allows mutual trust between parties or mutual reliance on a third party"[175] in the case of a dispute, to boost business transactions. It must be inferred that e-commerce platforms can only provide the necessary trust in the market if they can offer users an ODR mechanism that guarantees the execution of the result without entirely relying on the willingness of the losing party to voluntarily comply. In other words, the dispute resolution mechanism used by an e-commerce platform must enable aggrieved users to obtain effective redress, failing which they may leave the platform and join another one.[176]

The example of e-commerce shows that it is necessary to create a kind of self-enforcement mechanism implemented by the ODR platform that issues the decision in order to build a comprehensive private justice system.[177] Self-enforcement of the outcome of a dispute subject to ODR is, however, only possible if the ODR provider (*i.e.*, the company who administers and coordinates the ODR platform), or the e-commerce platform to which the ODR mechanism is linked, has the power to enforce its decisions. This presupposes that it has some power of control over a valuable resource.[178] For example, eBay has succeeded in setting up such a system by teaming up with payment service providers to keep control over the payments.[179] When a buyer wishes to be refunded, the seller is encouraged to negotiate a solution, whether privately on eBay's platform or with the help of an independent ODR provider.[180] If the negotiations are unsuccessful and the payment was executed with select payment methods – credit card, PayPal, Apple Pay, Google Pay, or a voucher – the buyer can access eBay's internal dispute resolution mechanism called eBay Money Back Guarantee. After reviewing the buyer's claim, eBay can decide to

174 Katsh and Rabinovich-Einy (n 160), 70–72.

175 Schultz (n 162), 78.

176 Koulu (n 169), 90.

177 About the notion of self-enforcement in the meaning of enforcement by private authorities, see Schultz (n 157), 4. See also Pietro Ortolani, "Self-Enforcing Online Dispute Resolution: Lessons from Bitcoin" (2016) 36 Oxford Journal of Legal Studies 595.

178 Schultz (n 156), 8; Perritt (n 137), 215.

179 See *e.g.*, Koulu (n 169), 76–78; Loebl (n 169), 4–7; Thomas Schultz, "eBay: un système juridique en formation?" (2005) 22 Revue du droit des technologies et de l'information 27.

180 *E.g.*, consumers domiciled in the European Union may submit a claim on the EU's ODR platform <https://ec.europa.eu/consumers/odr/>.

pay him or her back and enforce its decision thanks to credit card chargebacks, sometimes without even consulting with the seller.

Even if the combination of control over the payment method and the ODR mechanism produces an effective private enforcement mechanism, eBay's ODR mechanism is not self-reliant and the decisions it renders are not independent. On the one hand, the platform must resort to the services of an intermediary (such as PayPal) to execute its decisions and, on the other hand, the procedure is conducted entirely by eBay rather than by an independent third party with no financial interests. This can be problematic as eBay may serve corporate interests instead of justice, possibly to the detriment of some users. In short, eBay's model of conflict resolution is expedient and may be biased.

While eBay has implemented a form of private justice system, it is rare that an e-commerce platform or an ODR provider has the means to directly enforce the ODR outcome. Yet, it is recognised today that the ability to self-enforce online non-binding arbitration decisions is a key characteristic for ODR to be a real alternative to state justice.[181]

5 Implementation of Blockchain Dispute Resolution (BDR)

We have seen that, for the time being, state courts cannot guarantee access to justice in a reliable manner for disputes involving DAOs. Connecting factors have a difficult time locating matters of corporate law that concern the governance of DAOs and contractual relationships on the blockchain to which DAOs are parties. Universal jurisdiction could offer a solution if states agree to offer the protection of their courts to disputes with little or no link to their legal order. Similarly, a choice of court agreement could allow the parties to subject their contractual relations to a state jurisdiction. However, there remains the difficulty to locate the defendant when the parties involved benefit from pseudonymity in the blockchain environment and, in any case, the vast majority of DAOs do not have the capacity to be a party to the proceedings. Furthermore, even if a dispute involving a DAO can be brought before a state court, enforcement on the blockchain of the judgment is challenging when the losing party does not voluntarily comply. State enforcement authorities do not have the power to force a smart contract to execute in a certain way, nor can they freeze or seize crypto assets from a DAO or an on-chain actor.

181 Same opinion: Loebl (n 169), 36–37 and 66; Cortés (n 163), 150.

While these issues are critical in state courts, they are much less so if the dispute is resolved through an ODR mechanism because those systems of private justice can be configured in a much more flexible manner than traditional state justice. As with disputes related to online transactions, such as e-commerce disputes, the resolution of disputes involving DAOs can be entrusted to an ODR mechanism. New types of ODRs have been imported on the blockchain to use this technology for resolving disputes of blockchain actors (5.1). Technology plays a central role in those kinds of ODRs and can be viewed as an integral party to the dispute resolution process (5.2). Blockchain-based dispute resolution mechanisms can be designed in a way which addresses the risk of non-compliance that is structurally inherent[182] in any private justice system. The use of blockchain technology avoids the main drawback of most ODR systems, which is the lack of coercive means of enforcement. Smart contracts bring a significant innovation with respect to automatic execution of transactions. These can be exploited to set up dispute resolution mechanisms that allow for the self-enforcement of the decision to be carried out directly and automatically through the system (5.3). A private justice system incorporating a direct and automatic decision enforcement mechanism may seem expedient at first sight, but the authority to judge is based on the agreement of the disputing parties who have chosen this particular mode of dispute resolution (5.4).

5.1 *From ODR to BDR*

ADRs give access to a wide variety of opt-in private justice mechanisms that can be voluntarily chosen by the parties to a contract when they have a conflict, either at the time of the conclusion of the contract, or after the conflict has occurred. Where the parties choose to resolve their dispute privately through an ADR mechanism, the state loses its power to dispense justice. However, the state keeps a certain control over the delivery of justice at other stages of the dispute resolution process. Traditional ADRs such as arbitration cannot directly enforce their decisions and rely on state enforcement authorities when voluntary compliance is not met. In this case, the dispute resolution process falls under the supervision of the state judiciary in the enforcement procedure. Through its monopoly over the use of force, which is manifested by its power of enforcement, the state keeps control over justice in its territory even when the parties to a contract opt for private justice provided by an ADR mechanism.

182 Ortolani (n 130), 303.

ODR has been specifically introduced to cater for the needs of online users, especially in e-commerce. Some online platforms (*e.g.*, eBay) have found a way to acquire a certain degree of independence by directly executing their decisions with technology (*e.g.*, through credit card chargebacks) when the parties have contracted online using digital tools. This is possible when there is a close interface between the marketplace, the payment method and the ODR service.[183] In this regard, the ODR justice system challenges the monopoly of states over the use of force by directly enforcing its decisions through the use of technology. However, the state does not lose all control over the delivery of justice as the parties can initiate legal proceedings to review the private resolution of the dispute, in which case the competent state court may reach a different decision. As a result, even though the litigation is initially resolved privately and goes under the radar of the state, state control remains because the parties can still have recourse to state justice if they find the result of the private proceedings to be unjust or unfair.

New generation ODRs have been designed to meet the specific needs of contractual relationships arising in the digital environment of the blockchain. Developers have created decentralised dispute resolution mechanisms on the blockchain that are adapted to the immutability of smart contracts and the pseudonymity of on-chain actors. The authors refer to those blockchain-based ODRs as "Blockchain Dispute Resolution" (BDR) mechanisms (BDRs). BDRs are the only dispute resolution mechanisms that can effectively resolve disputes on the blockchain because they use that very infrastructure to function. As they operate in the blockchain environment, the parties to a contractual relationship on the blockchain can give a BDR mechanism the power to review the execution of their smart contract when a dispute occurs, in which case the result of the BDR mechanism is directly and automatically enforced. BDRs are therefore independent in their operation; that is, they do not need any state authority to dispense justice and execute their decisions, as this is done through technology. BDRs are also self-reliant because the execution of a decision is done automatically by the smart contract, without having to rely on a third party (*e.g.*, a credit card company), as the smart contract has direct power over the subject matter of the contract. But the characteristic that sets BDRs apart from all other types of ODRs is their autonomy. BDRs are decentralised entities that are operated and maintained by communities of participants

183 See Jia Wang and Lei Chen, "Regulating Smart Contracts and Digital Platforms – A Chinese Perspective," in Larry A. DiMatteo, Michel Cannarsa and Cristina Poncibò (eds), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (Cambridge University Press 2020), 183, 192–193.

who are organised in DAO structures. They are not linked to a state jurisdiction and thus benefit from the autonomy provided by the blockchain infrastructure. The decision-making process and the execution of decisions completely escape state oversight as no state can control a BDR mechanism and impose actions that go against its code or the will of its community. For example, state authorities cannot order a BDR mechanism to freeze crypto assets by means of a provisional or conservatory measure. As state authorities have no oversight power over BDRS and cannot enforce decisions on the blockchain either, the blockchain environment not only infringes the power of the state to dispense justice, but also the power of the state to review decisions.

5.2 *Technology in the Dispute Resolution Process*

Technology plays a central role when a dispute is resolved through an ODR mechanism. This has been made clear by UNCITRAL which defined ODR as a "mechanism for resolving disputes through the use of electronic communications and other information and communication technology."[184] ODR can be technology-assisted dispute resolution as well as technology-facilitated dispute resolution or technology-based dispute resolution mechanisms.[185] In the first generation of ODRS, information technology was used basically for communicating data (*e.g.*, emails used for communications). The dispute resolution process has been transferred entirely online in the second generation of ODRS where technological tools have been given an important place, notably by integrating software that employs algorithms and artificial intelligence into decision making.[186] Those are the models which are currently used to resolve e-commerce disputes.

---

184 UNCITRAL, *Technical Notes on Online Dispute Resolution* (United Nations 2017), para. 24, available at <https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/v1700382_english_technical_notes_on_odr.pdf> accessed 28 June 2023.

185 Mohamed S. Abdel Wahab, Ethan Katsh and Daniel Rainey, "Introduction," in Mohamed S. Abdel Wahab, Ethan Katsh and Daniel Rainey (eds), *Online Dispute Resolution: Theory and Practice* (eleven 2012), 1, 3. See also Loebl (n 169), 3–4.

186 See Adesina Temitayo Bello, "Online Dispute Resolution Algorithm: The Artificial Intelligence Model as a Pinnacle" (2018) 84 Arbitration – The International Journal of Arbitration, Mediation and Dispute Management 159. See also Arno R. Lodder and John Zeleznikow, "Artificial Intelligence and Online Dispute Resolution," in Mohamed S. Abdel Wahab, Ethan Katsh and Daniel Rainey (eds), *Online Dispute Resolution: Theory and Practice* (eleven 2012), 61, 73–75; Aura Esther Vilalta, "ODR and E-Commerce," in Mohamed S. Abdel Wahab, Ethan Katsh and Daniel Rainey (eds), *Online Dispute Resolution: Theory and Practice* (eleven 2012), 113, 116–118, for a distinction between automated and assisted negotiation, online mediation, online conciliation, and online arbitration.

The central role of technology in the dispute resolution process of ODRs has been highlighted by the metaphor of the "fourth party."[187] Technology assists both disputing parties as well as the third party involved in the dispute resolution process (*e.g.*, the arbitrator) to find a consensus or to make a decision.[188] Technology can even take the place of the third party. For example, technology replaces the mediator in the case of automated negotiation decision-making.[189] Arno Lodder stated that "[b]asically, technology in ODR can be applied for the following purposes: supporting the communication, supporting the exchange of documents and information, supporting decisions, and making decisions."[190] This author has gone further by also acknowledging the role of the ODR provider. He called the ODR provider the "fifth party" of ODR,[191] while noting that "[t]he fifth party is present only if either the technology was developed for supporting the resolution of disputes, or the provider aims to deliver tools that help the parties in solving the conflict."[192]

BDRs are a third generation of ODR that are characterised by the use of blockchain technology. They carry out the whole dispute resolution process in the digital environment of a blockchain and rely on smart contracts from the initiation of the dispute resolution procedure to the actual resolution of the dispute and, finally, the enforcement of the outcome. A smart contract is used by the disputants to submit their dispute to the BDR mechanism and other smart contracts are used to resolve the dispute within the BDR mechanism and ultimately execute the decision. Blockchain technology plays such a key role in the dispute resolution process that it must truly be considered as playing the role of a fourth party. The fourth party goes beyond the metaphor in ODR to become a reality in BDR. We can deduce that the fourth and fifth parties are one and the same in a BDR mechanism.

187 Ethan Katsh and Janet Rifkin, *Online Dispute Resolution: Resolving Conflicts in Cyberspace* (Jossey-Bass 2001), 93–116. See also Katsh and Rabinovich-Einy (n 160), 11.

188 Ethan Katsh, "Online Dispute Resolution: Moving Beyond Convenience and Communication," in James R. Silkenat, Jeffrey M. Aresty and Jacqueline Klosek (eds), *The ABA Guide to International Business Negotiations – A comparison of Cross-Cultural Issues and Successful Approaches* (3rd edn, ABA Book Publishing 2009), 235, 238.

189 *E.g.*, the blind-bidding system of dispute resolution which is used by Cybersettle. See Arno R. Lodder and John Zeleznikow, *Enhanced Dispute Resolution Through the Use of Information Technology* (Cambridge University Press 2010), 82–84.

190 Arno R. Lodder, "The Third Party and Beyond. An Analysis of the Different Parties, in particular The Fifth, Involved in Online Dispute Resolution" (2006) 15 Information & Communications Technology Law 143, 152.

191 Lodder (n 190).

192 Lodder and Zeleznikow (n 189), 81.

5.3 *On-Chain Enforceability of BDR*

The dispute resolution process of a BDR mechanism is conducted entirely on the blockchain and is configured in such a way that it can be performed using smart contracts. Given these properties, the use of a BDR mechanism does not require the parties to disclose their real identity and pseudonymity can be upheld. All operations on the blockchain are linked to a public key which points to the owner's crypto wallet, whether it is signing a smart contract, joining a DAO, or transferring cryptocurrencies and other crypto assets. Since the public key serves as identification in the blockchain environment, a BDR mechanism can enforce any decision upon the parties without their identity being disclosed.

Any decision must be enforceable according to the properties of the smart contract. In general, disputes are settled in a binary way by choosing between two options. For example, if the contentious smart contract is a governance proposal in a DAO, the decision stemming from the BDR mechanism must either stop the proposal or let it go through. Or, if the contentious smart contract is a payment in cryptocurrencies for the delivery of a service, the decision stemming from the BDR mechanism must either let (part of) the payment go through or cancel the payment all together. As a result, existing BDRs do not deal with all types of disputes and are limited to cases where the disputing parties are in a position to agree on two options to resolve their dispute. However, this binary situation is not common in everyday disputes. The resolution of a dispute usually involves a succession of small decisions according to a reasoning process that can hardly be reproduced in a binary way. But it cannot be excluded that more complex BDRs will be developed to allow more complex decisions to be taken and executed. One could imagine, for example, that the decision-making process is composed of a series of smart contracts triggered according to the decision taken at the previous level. For the time being, the BDRs are still limited to conflict resolution mechanisms configured in a binary way to clearly determine which disputing party is right and which is wrong.

One of the advantages of smart contracts is that any action on the blockchain (*e.g.*, the transfer of cryptocurrencies and other crypto assets) can be conditioned to a set of predefined rules. It is possible to take advantage of this property of smart contracts to make decisions that are self-executable. Here, the effectiveness of the dispute resolution process does not rely on the willingness of the parties to comply with the decision. There is therefore no need to use mechanisms that incentivise parties to voluntarily comply, which is the case in most ODRs.[193] Hence, an essential feature of BDRs is their ability to

193 Some ODRs such as eBay's Money Back Guarantee keep control over the payment in order to have the means to enforce a decision in case of a conflict (see *supra* chapter 4.2.2).

directly and automatically enforce their decisions on the blockchain itself by using smart contracts, which allows the parties to obtain the enforcement of decisions without having to rely on the assistance of coercive state authorities. This makes BDRs independent and self-reliant dispute resolution mechanisms, which is a major improvement over ODRs that do not use this technology.[194] In other words, blockchain technology brings the certainty of enforcement of the ruling.[195]

However, the power of enforcement of BDRs is delimited by the constraints of the technology. The decisions arising from a BDR mechanism must be enforceable through a smart contract on the valuable resources that have been submitted in its technological environment. The scope of the power of enforcement of a BDR mechanism is limited to cryptocurrencies or other crypto assets that have been placed by the parties within its power by means of a smart contract. For example, a smart contract that submits to the jurisdiction of a BDR mechanism can be programmed in such a way that cryptocurrencies are transferred automatically from one account to another when pre-set conditions are satisfied (*e.g.*, "if A is right, then 10 ETH are transferred to A's account"). Until the smart contract executes itself, the cryptocurrencies (10 ETH) are placed by the parties within the jurisdiction of the BDR mechanism. This statutory deposit is an essential element of the procedure before BDRs and it does not necessarily have to take the form of a deposit of valuable resources. The "statutory deposit" may also consist in the fact that the parties give the BDR mechanism the power to perform a particular action on the blockchain. For example, when the dispute is about some action related to the governance of a DAO, such as a proposal to implement a fork, a smart contract can temporarily block the proposal and then let it go through (or not) in accordance with the BDR mechanism's decision. If the BDR mechanism is not able to stop the transfer of the disputed assets or the execution of the disputed proposal, its power to rule on the dispute is hampered by the fact that the system will not be able to directly and automatically enforce its decision. When the decision rules on elements that are outside of the BDR mechanism's technical reach, for example by ordering the transfer of off-chain assets, the execution of the decision

---

However, those ODRs rely on third parties (*e.g.*, payment service providers) that may charge additional fees to the losing party, which amounts to a double penalty.

194 See *supra* chapter 5.1.

195 Federico Ast and Bruno Deffains, "When Online Dispute Resolution Meets Blockchain: The Birth of Decentralized Justice" (2021) 4.2 Stanford Journal of Blockchain Law & Policy 241, 244.

cannot be guaranteed. Therefore, BDRs are best suited for decisions that are to be enforced exclusively on-chain.

The main difference between BDRs and ODRs that do not use blockchain technology lies in the fact that BDRs are part of an economic system in which there are valuable resources. A BDR mechanism can be granted "jurisdiction" (*i.e.*, power) over some cryptocurrencies or other crypto assets that are part of the blockchain environment in which it is implemented, the same way that assets on the territory of a state are under the jurisdiction of the judicial authorities of that state. The BDR mechanism exercises its power of jurisdiction autonomously as no state can interfere with the crypto assets under its jurisdiction. It is also independent and self-reliant in the enforcement of its decisions as the BDR mechanism has the power to directly and automatically transfer the subject matter of the dispute (*i.e.*, valuable resources that are in its power) to the winning party at virtually no cost and without the involvement of a third party or coercive state authorities. By producing decisions that can be automatically self-enforced by the system, BDRs represent the culmination of a private justice system.

5.4 *Jurisdiction Based on Consent*

As with other forms of ODR, the jurisdictional competence of a BDR mechanism necessarily stems from the will of the parties to place their relationship within its jurisdiction. There must be an agreement on the choice of a BDR mechanism which is to have jurisdiction to settle any disputes that have arisen or may arise in connection with a particular relationship. The choice of BDR cannot be established unilaterally: it must result from the consent of each of the disputing parties, the same way as the choice of a state court must result from a choice of court agreement or an arbitration agreement.

The "choice of court clause," or rather "opt-in clause," containing the agreement of the parties to subject any dispute to a BDR mechanism's jurisdiction, must be encoded in one of the smart contracts governing the relationship between the parties.[196] The parties may also agree to entrust a dispute that has already arisen to the jurisdiction of a BDR mechanism by generating a specific smart contract. For example, the parties may create a smart contract that elects the BDR mechanism to decide between programmed possible outcomes. In both cases, the smart contract enables the activation of an external dispute resolution mechanism.

196 As a reminder, we only consider smart contracts that are the legal contracts themselves. See *supra* chapter 3.3.

The dispute resolution mechanism can also be directly integrated into the smart contract.[197] In this situation, the dispute resolution mechanism is internal to the smart contract. For example, a smart contract may be linked to a multi-signature wallet which allows the intervention of a third party to release the cryptocurrencies deposited in the wallet.[198] If a dispute occurs, the third party has the power to decide where the cryptocurrencies stored in the wallet shall be transferred. This type of dispute resolution mechanism will not be further analysed as it falls outside the scope of BDRs as defined above,[199] which are decentralised and autonomous mechanisms external to the smart contract.

In the case of disputes related to the governance of a DAO, when the code of the DAO incorporates an opt-in clause submitting any dispute among the members or between the DAO and its members to a BDR mechanism, this clause is to be regarded as an agreement to which all members have assented. The opt-in clause shall be considered as binding on all members of the DAO, who can be deemed to have implicitly accepted the jurisdiction of the BDR mechanism at the time they acquired governance tokens of the DAO, along with the other provisions specified in the DAO's code. This rule is generally accepted in the case of a choice of court clause[200] or an arbitration clause[201] in the bylaws or articles of association of a company. In any case, the members are bound by the opt-in clause through the DAO's code, and there is no technical way they can get around it in case of a dispute. In the authors' view, the principle that all members of a DAO have agreed that a dispute arising among them or between them and the DAO is to be decided by a BDR mechanism is all the easier to accept because the DAO's code (in which the opt-in clause is included) is freely accessible online on the blockchain's ledger.

With regard to contractual relations between a DAO and third parties, the opt-in clause can be encoded in the smart contract governing the relationship

197 *E.g.*, a draft bill on smart contracts of the State of Wyoming of 2019 (19LSO-0049) had a provision (40-28-102) under which "(a) A smart contract [...] shall, as a condition of enforceability in this state, be accompanied by a resolution plan agreed upon by the parties to the contract. [...] The requirements of this section may be executed through the code or programming language of a smart contract or may accompany the contract through any readily accessible means agreed upon by the parties to the contract. (b) [...]." This bill has not yet entered into force.

198 See Ortolani (n 86), 434–435.

199 See *supra* chapter 5.1.

200 See *e.g.*, Trevor Hartley, *Choice-of-court Agreements under the European and International Instruments* (Oxford University Press 2013), 152–154.

201 See *e.g.*, Kaufmann-Kohler and Rigozzi (n 145), para. 3.88–3.90. See also the new Art. 178 para. 4 of the PILA, under which the provisions related to international arbitration "apply by analogy to an arbitration clause [...] in articles of association."

between the parties. The question arises as to whether the choice of BDR can also result directly from the code of the DAO. To what extent can such an opt-in clause be considered as binding on third parties when they have not acquired governance tokens of the DAO? From a corporate law point of view, it is *a priori* impossible to presume that third parties have assented to a choice of court or arbitration clause in the bylaws or articles of association of the company. It is regular business for third parties to enter into commercial relations with companies without knowing the content of their bylaws or articles of association. In such cases, third parties are not bound by a choice-of-court or arbitration clause that could be found in the bylaws or articles of association. This analogy with corporate law has its limits given that, unlike the bylaws or articles of association of a company, the rules of management and governance of DAOs are systematically freely accessible on-chain and can be consulted at any time by anyone. Therefore, it could be assumed that any third party entering in business relations with a DAO is deemed to be aware of the rules in the DAO's code and in particular the existence of an opt-in clause referring to BDR since the software code is public and can be freely consulted on the blockchain. In this case, we should come to the conclusion that an implied consent for the BDR mechanism's jurisdiction exists when it is programmed in the DAO's code. This analysis is reinforced by the fact that if the code of the DAO submits to the jurisdiction of the BDR mechanism for all its smart contracts with third parties, either there is no technical way for the parties to get around it in case of a dispute, as the smart contract will self-execute.

By requiring that anyone who deals in some way with a DAO should be aware of the technicalities in the DAO's code such as for example opt-in clauses, one assumes that any third party is able to read the software code, which is not something everyone can do. For this reason, it is the opinion of the authors that DAOs which have an automatic opt-in clause submitting any dispute to BDR should inform, in a comprehensive way, potential DAO token buyers and third parties entering into commercial transactions with the DAO that any dispute which may arise in their relationship with the DAO will be resolved by the BDR mechanism, in accordance with the DAO's code. This information should be included, for example, in the DAO's white paper, which should be published on a public platform and be publicly available. In this manner, it can be assumed that anyone who has a relationship with the DAO knows, or ought to know, that it is bound by the opt-in clause which is part of the membership into the DAO or part of the contractual agreement with the DAO. Failing that, the DAO should at least inform potential members or contracting parties in natural language of the existence of such a dispute resolution clause in its code. It is of particular importance that DAOs be fully transparent with the content

of their code as third parties that do not have special knowledge in computer coding could end up being bound in a relationship with a DAO without fully understanding the scope of that relationship. And the characteristics of smart contracts would prevent them from simply withdrawing from that relationship. DAOs that do not respect basic principles of transparency could be indirectly sanctioned by losing their reputation. In any case, a BDR mechanism should refuse to exercise its jurisdiction when a contracting party to a smart contract demonstrates that it was not properly informed about the existence of such a dispute resolution clause in the DAO's code. Consent should not be disregarded even in the technologically driven environment of the blockchain. As justice providers, BDRs have the responsibility to prevent abusive conduct when possible.

6 Resolving Disputes Involving DAOs by Means of BDR

With the development of the crypto economy through DeFi and other types of Decentralized Applications (dApps), it is of paramount importance that DAOs and other actors of the crypto environment be offered access to justice, as state courts are often powerless when faced with blockchain technology. BDRs are in principle the only way DAOs, their members, and their contracting parties can access justice in case of a dispute. As many DAOs do not have legal capacity and cannot sue or be sued before state courts, BDRs represent their primary access to justice. However, the exceptional case of a dispute between a regulated DAO and an off-chain actor must be reserved. This type of case can be settled by state courts, at least in states where the DAO has the capacity to sue and be sued in the same way as other forms of companies. Only the enforcement of the decision on cryptocurrencies, other crypto assets, or on the DAO's governance could be problematic.[202]

BDRs allow on-chain and off-chain actors to resolve their disputes with platforms that are adapted to the crypto environment. Most BDRs[203] are specifically configured to allow DAOs to take part in proceedings. Those BDRs

202 See *supra* chapter 3.5.

203 For an overview of recent BDR projects, see *e.g.*, Yann Aouidef, Federico Ast and Bruno Deffains, "Decentralized Justice: A Comparative Analysis of Blockchain Online Dispute Resolution Projects" (2021) 4 Frontiers in Blockchain <https://www.frontiersin.org/articles/10.3389/fbloc.2021.564551/full> accessed 28 June 2023; Michael Buchwald, "Smart contract dispute resolution: the inescapable flaws of blockchain-based arbitration" (2020) 168 University of Pennsylvania Law Review 1369, 1384–1393; Rabinovich-Einy and Katsh (n 86), 59–71; Metzger (n 86), 88–100; Allen, Lane and Poblet (n 86).

incorporate decision-making processes which are based on crypto-economic mechanisms that lead to decisions by consensus (6.1). The first operational BDR was specifically developed to resolve disputes of a contractual nature for relationships created on the blockchain with smart contracts. As a result, on-chain actors who may be pseudonymous or exist only in the digital environment, but possess cryptocurrencies or other crypto assets, have the opportunity to access justice when contracting on the blockchain, while off-chain actors venturing in the crypto economy are offered a way to securely contract with on-chain actors and access justice in case of a dispute (6.2). Additionally, like any organised entities, DAOs are also prone to conflicts pertaining to their governance. A second BDR mechanism has been launched to specifically allow DAO members to have proposals with regard to the governance of the DAO submitted by their peers to be assessed by a jury in order to determine whether litigious proposals are in line with the DAO's goals and values and to block them from being voted on if necessary (6.3).

6.1 *Decision-making Process in BDRs*

At the time of writing, Kleros[204] and Aragon Court[205] are two BDRs that are operational for resolving disputes on the blockchain and are accessible to DAOs. Kleros was launched on the Ethereum blockchain in July 2018 and is, as such, the first BDR platform in operation.[206] Aragon Court was launched in November 2019, also on the Ethereum blockchain, with a mechanism inspired by the one of Kleros.[207] Those two BDRs share the common particularity of relying on crowdsourcing in their dispute resolution process. The characteristic feature of crowdsourcing is that the dispute is resolved by a jury composed of people who are not necessarily legally qualified, but who can take a stand on a dispute based on personal experience and technical qualifications. The emergence of crowdsourcing in the resolution of disputes has already been observed ten years ago by van den Herik and Dimov in ODRs developed for e-commerce.[208] These

204 About Kleros, see Clément Lesaege, William George and Federico Ast, "Kleros Yellow paper" (March 2020), <https://kleros.io/yellowpaper.pdf> accessed 28 June 2023.

205 About Aragon and Aragon Court, see "Aragon White paper" (*GitHub*, 18 July 2019) <https://github.com/aragon/whitepaper> accessed 28 June 2023.

206 More than 900 disputes have already been resolved by Kleros at the time of writing, with more than 800 registered jurors.

207 Aouidef, Ast and Deffains (n 203), 3.

208 Jaap van den Herik and Daniel Dimov, "Towards Crowdsourced Online Dispute Resolution," in S. Kierkegaard and P. Kierkegaard (eds), *Law Across Nations: Governance, Policy and Statutes* (International Association of IT Lawyers 2011), 244–257, available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1933392> accessed 28 June 2023. These

authors highlighted the fact that some ODRs use the wisdom of the crowd to resolve a dispute, the crowd being composed of (some of) the members of the online community.[209] Using a jury of peers is considered an appropriate way to obtain a decision that reflects the opinion of a whole community.

This model has been adopted by Kleros and Aragon Court and implemented in a way that takes full advantage of blockchain technology. Jurors of those two BDRs are selected to judge a case at random from a pool of jurors who have bought their position by acquiring native tokens (*i.e.*, tokens from the platform). Jurors must stake some native tokens in order to show their interest with the case. The chances of being chosen as a juror increase with the amount of tokens a juror has staked. The decision-making process is designed so that jurors have an economic incentive to make a decision by consensus. In order to incentivise the vote for the "right" solution, Kleros and Aragon Court have the particularity of placing an economic risk on the jurors who voted for the unsuccessful resolution of the dispute. Jurors are remunerated only if they voted with the majority. Each of the majority jurors receives a portion of the fees that have been paid by the parties (called "arbitration fees") and, apparently, a portion of the stakes of the minority jurors. Jurors have therefore a double economic incentive to vote consistently with what they predict the majority vote will be, as they cannot only win money but also possibly lose money if they vote with the minority of jurors.

Kleros developers have explicitly referred to economic theories such as game theory when designing their dispute resolution mechanism.[210] The main economic mechanism used currently is the Schelling Point (or focal point).[211] The Schelling Point is, in game theory, a solution to which the participants in a game who cannot communicate with each other will tend to adopt because they think that this solution presents a characteristic which will make the other

---

authors called an ODR mechanism using crowdsourcing as a part of the dispute resolution process "Crowdsourced Online Dispute Resolution (CODR)." Other authors use the term "mob justice": Schmitz and Rule (n 86), 117; or "peer-to-peer arbitration": Michael Abramowicz, "Cryptocurrency-Based Law" (2016) 58 Arizona Law Review 359, 405.

209 Using the wisdom of the crowd to decide disputes has already been incorporated into ODRs in e-commerce. Already in 2008, eBay set up the eBay Users' Community Court in India to resolve disputes over buyer ratings (this ODR mechanism is no longer in operation). See Colin Rule and Chittu Nagarajan, "The Wisdom of Crowds: The eBay Community Court and the Future of Online Dispute Resolution," ACResolution (Winter 2010), available at <http://colinrule.com/writing/acr2010.pdf> accessed 28 June 2023.

210 About the game theory mechanisms used in such BDR, see Clément Lesaege, Federico Ast and William George, "Kleros – Short paper v. 1.0.7" (September 2019) <https://kleros.io/whitepaper.pdf> accessed 28 June 2023.

211 Thomas C. Schelling, *The Strategy of Conflict* (2nd edn, Harvard University Press 1980), 57.

participants choose it too. Under this theory, "if everyone expects everyone else to vote truthfully, then their incentive is to also vote truthfully in order to comply with the majority, and that's the reason why one can expect others to vote truthfully in the first place."[212] Jurors of Kleros seek the "consensual truth about the dispute" (*i.e.*, the Schelling Point) in order to vote with the majority and get a remuneration.[213] Just as Kleros, Aragon Court is designed as a consensus reaching mechanism relying on economic theories, such as game theory and the Schelling Point model. The designers of these BDRs clearly assume that the dispute resolution process is built primarily on economic incentive mechanisms that motivate jurors to anticipate what the decision of the majority of jurors will be and vote in favour of this decision.[214] This dispute resolution process is not surprising considering that blockchain technology is founded on consensus mechanisms allowing the shift of trust onto the architecture of the computer system itself.[215] Furthermore, the whole architecture of public blockchains is based on crypto-economic incentives, which encourage participants to co-operate and create the value that will ensure the success of the blockchain by giving them financial rewards. The dispute resolution processes of Kleros and Aragon Court seem therefore adapted to the particularities of the crypto environment and are likely to be accepted by on-chain actors.

Economic profit is directly linked to good reputation, as the more tokens jurors stake, the more the system assumes that they have the ability to judge with the majority and earn more tokens. The stakes of the jurors are an indication not only of their reputation, but also of their competence. In accordance with the principles of game theory applied in the dispute resolution mechanism, jurors' competence is essentially measured by their ability to anticipate the decision that will be made by the majority of jurors. This capacity is economically encouraged by the system because the BDR mechanism has an interest in making consensus decisions. As the reputation of each juror increases, the reputation of the BDR mechanism also increases as consensus is more easily reached.[216] The more the reputation of the BDR mechanism increases, the more the value of the platform's native tokens increases and the more the

212 Aouidef, Ast and Deffains (n 203), 4.

213 Ast and Deffains (n 195), 249–251.

214 See *e.g.*, Facu Spagnuolo, "Crypto-economics considerations" (*GitHub*, 21 November 2019) <https://github.com/aragon/aragon-court/tree/v1.0.0/docs/3-cryptoeconomic-considerations> accessed 28 June 2023.

215 See *e.g.*, Riva (n 2), 603–605; De Filippi and Wright (n 13), 42–43.

216 See Jack Gane, "Juror Pre-activation Guide" (*Aragon Org Blog*, 7 January 2020) <https://blog.aragon.org/juror-pre-activation-guide/> accessed 28 June 2023. The link between participant reputation-staking and DAO valuation was highlighted by Kaal (n 19), 38–40.

jurors will benefit economically from earning native tokens.[217] It is therefore not surprising that the behaviour of the jurors receives more attention from the designers of BDRs such as Kleros and Aragon Court than the behaviour of litigants.

This reputational model diverges from that of traditional dispute resolution mechanisms. Many ODR providers have tried to address the risk of non-execution of their decisions by implementing social and economic incentives that favour voluntary compliance by the losing party as, contrary to BDRs, automatic execution is rarely available in ODRs.[218] Reputational risk has proven to be an effective means of addressing the lack of enforceability of the outcome of ODRs. However, in BDRs, reputational risk is found in the decision-making process, not in the enforcement of the decision. There is thus a transfer of reputational risk from the losing party (in ODRs) to the "losing" jurors (in BDRs). While jurors who rule in the majority gain a good reputation, this is not the case for those who have been outvoted. A minority juror therefore suffers both economically and in terms of reputation. In certain BDRs, the reputation of jurors is already factored into the selection process of potential jurors.[219]

However, this does not mean that the reputation of the disputing parties is not likely to be tainted in proceedings submitted to BDR. For example, if the proposal containing the action being planned by a DAO is successfully challenged by one of its members in Aragon Court, the DAO suffers reputational damage because the jurors have recognised that it was planning a bad action. The reputation of the parties to a dispute is always, to some extent, subject to damage when the existence of the dispute is known, as will generally be the case in a dispute involving a DAO.

6.2 *Disputes of a Contractual Nature*

When a dispute related to the execution of a smart contract arises, the resolution of the dispute is entrusted to the BDR mechanism chosen by the parties in

217 However, the more consensus there is between the jurors, the less each majority juror earns from the stakes of the minority jurors and the arbitration fees.

218 See *supra* chapter 4.2.2.

219 The arbitration fees in Aragon Court are proportional to the amount of reputation of the jurors; see Aragon White paper (n 205). OpenBazaar already uses a model to select "moderators" based on their reputation; see OpenBazaar, "Verified moderators" (*Medium*, 11 January 2018) <https://medium.com/openbazaarproject/verified-moderators-c83ea2f2c7f3> accessed 28 June 2023. The project Jur, which has not been launched yet, allows for jurors to be peer-reviewed, which leads to a ranking of jurors according to their reputation; see Jur, "Jur Documentation Hub" <https://gitbook.jur.io/jur-documentation/> accessed 28 June 2023. See already Kaal and Calcaterra (n 82), 150.

the smart contract. The third party appointed by the BDR mechanism, who is in charge of rendering a decision, must analyse the smart contract, the reason why it was not executed or improperly executed, and decide on the basis of its assessment of the facts and the evidence provided by the parties which party is right.

Kleros may be chosen by the parties to a smart contract to settle disputes arising from the non-execution or improper execution of the smart contract. When developing their smart contract, the parties must define and implement the dispute parameters which determine how and when a dispute resolution procedure can be initiated. Once a dispute occurs, the parties must determine the two options available for jurors to vote on (*e.g.*, [1] "A is right," [2] "B is right") and the behaviour of the smart contract after the resolution of the dispute for each possible option (*e.g.*, [1] "if A is right, then 10 ETH are transferred to A's wallet," [2] "if B is right, then 10 ETH are released"). When the dispute concerns the transfer of cryptocurrencies or other crypto assets, those assets must be placed by the parties within the power of the BDR mechanism. This is usually automatically done by the smart contract that defines their contractual relationship through a clause that works in a similar way as an escrow arrangement. When this is not the case, the parties must accept to transfer the disputed cryptocurrencies or crypto assets within the power of the BDR mechanism with a subsequent smart contract. This second option might be harder to achieve as it implies that both parties voluntarily subject themselves and the disputed assets to the power of the BDR mechanism after the dispute. Once the jurors are presented with the two options, they vote in favour of one of the options to resolve the case after having assessed the arguments and evidence submitted by each of the parties. They vote *ex aequo et bono* on the basis of their technical knowledge and personal experience. The votes are not visible to the other jurors or to the parties so as to prevent one juror from being influenced by the vote of another. Parties can appeal an indefinite number of times, each new appeal instance having twice the previous number of jurors plus one and the arbitration fees increasing at each instance. When there are no more appeals, the decision is final and is directly and automatically enforced through the computer system.

The fact that the parties to the dispute are pseudonymous on-chain actors does not prevent the resolution of the dispute.[220] With Kleros, the parties must not be identified to either take part in the proceedings or enforce the decision. They must only sign the smart contract – which has a clause that grants the BDR mechanism jurisdiction over their contractual relationship – with their

220 See *supra* chapter 5.3.

public key. This requirement is within the means of any DAO or person with a crypto wallet. As for the dispute resolution procedure and the enforcement of the decision, they are automatically initiated by the smart contract and Kleros.

Surprisingly, Kleros is not limited to disputes involving on-chain actors. This BDR is also positioned as an alternative to traditional ODRs whose methods are too slow or too expensive.[221] Kleros offers its services to solve disputes arising between two off-chain actors in relation with the execution of a traditional contract when the parties seek a "fast, inexpensive, transparent, reliable [...] dispute resolution mechanism that renders ultimate judgments."[222] For example, a dispute between a cruise company and a couple who had booked an all-inclusive river cruise has been solved by Kleros.[223] In this case, the jurors had to decide between awarding the couple 70% of the price of the cruise, which was the behaviour they sought in case they won, or awarding the couple a small payback and a voucher for a future cruise, which was the behaviour the cruise sought in case it won.

It should not be forgotten that the ability of BDRs to resolve disputes and to enforce the outcome is limited by technology. At this point, disputes that come to Kleros must be resolvable in a binary way so as to permit the automatic self-enforcement of the decision using a smart contract. In the river cruise case, the jurors had to choose between the offer submitted by each party to settle the dispute, and it is unclear whether the parties had placed cryptocurrencies within the power of the BDR mechanism in order for the decision to be automatically enforced, or if the decision had to be executed off-chain by the cruise company. In the latter case, the system's automatic enforcement mechanism would not have been used and the parties would have missed out on the main benefit of resolving a dispute through BDR.[224] The couple would have primarily relied on the voluntary execution of the decision by the cruise company, with a motivation based mainly on reputation. And if the risk of damage to the reputation would have not been enough to push the cruise company to comply with the decision, the couple would have had to seek the assistance of state authorities to obtain the enforcement of Kleros's decision by force.

221 Aouidef, Ast and Deffains (n 203), 4.

222 In the words of Lesaege, George and Ast (n 204), 1. About the use of Kleros to resolve traditional off-chain disputes, see Dmitry Narozhny, *Due Process in Kleros Consumer Dispute Resolution* (Kleros 2019) <https://ipfs.kleros.io/ipfs/QmdH7vuFVATLqdsvWXBBq38fUX2jRp7tbiQ1MvBr8SDxBc> accessed 28 June 2023.

223 Case 541: <https://resolve.kleros.io/cases/541> accessed 28 June 2023.

224 See *supra* chapter 5.3.

However, it is more than uncertain whether a decision from Kleros can be recognised and enforced in a state jurisdiction.[225]

6.3 *Disputes Related to the Governance of DAOs*

Disputes related to the governance of a DAO usually concern decisions regarding the management and operations of the entity, such as allocation of resources, entry and exit of members, issuance of tokens, launch of a crowdfunding campaign, or ethical issues related to the governance. If a DAO and its members are bound to a BDR mechanism through an opt-in clause in the DAO's code, disputes related to the governance of the DAO are ruled by that BDR mechanism.[226] As outlined in the Aragon White paper, "[e]ach Aragon organization [*i.e.*, DAO] exists as a set of smart contracts that define the organization's stakeholders and their associated rights and privileges. However, some rights and privileges require subjective constraints that cannot be encoded in a smart contract directly."[227] It is to solve disputes arising in connection with this type of matter that the Aragon Court was launched.

Aragon Court uses crowdsourcing as a part of the dispute resolution process and follows a procedure that has several similarities with that of Kleros, even if the two procedures are not fully identical. In Aragon Court, the jurors are asked to either block a proposal from being voted on by the community, or to let it go through. The jurors get access to a description of the claim and evidence provided by each party to determine whether the proposal is in line with the DAO's bylaws, goals or ethical values. The final ruling is automatically executed by definitively blocking the disputed proposal or letting it be voted on, and by distributing the rewards and penalties to the jurors.

To illustrate Aragon Court's procedure, let's take as an example the case where a group of members in a DAO submit a proposal to the DAO regarding the launch of a crowdfunding campaign. A DAO member who believes that the action being proposed is not in line with the DAO's goals or values and fears that the proposal will gather enough votes to pass, may block the proposal from being voted on by bringing a dispute to Aragon Court. Selected Aragon Court jurors must choose between two options ([1] "allow the proposal regarding the crowdfunding campaign to be voted on," [2] "block the proposal regarding the crowdfunding campaign to be voted on"). The option which gets the majority of votes is directly and automatically executed through the smart contract.

225 See *infra* chapter 7.3.
226 See *supra* chapter 5.4.
227 See *supra* n 205.

The enforcement of the jury's decision is only possible if the DAO's code allows the decision to be self-enforced, which implies a technological connection between the DAO and Aragon Court. In other words, the dispute resolution mechanism can only be effective if the enforcement of the outcome is within technical reach of the court. In order to block a proposal before Aragon Court, the DAO must be under its jurisdiction. The code of all DAOs constituted on the Aragon platform automatically refer to Aragon Court for the resolution of disputes arising among the members of the DAO or between the DAO and its members. Other DAOs that run on the Ethereum blockchain can also refer to Aragon Court by implementing a connection in their code. This connection is necessary as Aragon Court does not have the technical power to enforce its decisions on DAOs that are outside its network. When the disputed proposal concerns the management or operation of a DAO that was not constituted on the Aragon platform or to which no connection was made to Aragon Court in its code, a decision of Aragon Court could not technically be directly and automatically enforced. If Aragon Court is not given the power to block or unblock the disputed proposal, it has *de facto* no power to rule on the dispute. This limitation on its enforcement power is a flaw in the effectiveness of this dispute resolution mechanism that could be detrimental to it.

While it is unequivocal that maverick DAOs can subject disputes related to their governance to BDR, it remains to be determined whether regulated DAOs – which are DAOs that have a corporate body –[228] can subject that kind of dispute to the jurisdiction of a BDR mechanism such as Aragon Court. The particularity of disputes related to the governance of a regulated DAO is that they can relate either to the management and governance rules of the DAO set out in its code, or to those set out in the corporate law of the state in which the regulated DAO is incorporated (*i.e.*, its *lex societatis*).

When the dispute concerns a governance rule embodied in the code of the regulated DAO and governing the DAO as such, the dispute is best dealt with by an Aragon Court-type BDR mechanism. In this case, the jurisdiction of the BDR mechanism is in principle based on the opt-in clause in the regulated DAO's code,[229] or, in the case of regulated DAOs created on Aragon's platform, dispute resolution through Aragon Court is an integral part of the DAO's code. The disputing parties can take advantage of the power of the BDR mechanism to enforce the decision directly and automatically.

On the other hand, when the dispute concerns a rule found in the corporate law of the state in which the DAO is incorporated, these rules apply primarily to the corporate body of the DAO (*e.g.*, a Vermont BBLLC). Such a dispute falls

228 See *supra* chapter 2.3.2.

229 See *supra* chapter 5.4.

within the jurisdiction of the authorities of the state in which the DAO was incorporated, whose jurisdiction may be based, in this case, on the seat of the company or possibly a choice of court clause in the bylaws or articles of association of the regulated DAO. The power to enforce a decision on the corporate body of the DAO (*i.e.*, in principle the registered agent of the regulated DAO) is solely in the hands of the state authorities of the place of incorporation of the regulated DAO.[230] A BDR mechanism would not have the technical means to enforce a decision on such matters.

7 What is Effective and Fair Justice in the Crypto Economy?

The last chapters have shown us not only that the crypto environment has developed an economic ecosystem in which DAOS play a central role, but also that it has yielded dispute resolution mechanisms that can resolve a vast array of disputes – from contractual relationships to governance disagreements within DAOS – and are capable of self-enforcing the decisions they render through technology. But in order to be seen as legitimate authorities by the users who are submitted to their decision-making power, BDRS need to be trustworthy institutions of the blockchain environment. This can only be achieved if they can provide effective and fair justice.

BDRS that incorporate an enforcement mechanism provide effective access to justice, in the sense that actors of the crypto economy can choose to resolve their conflicts with a dispute resolution mechanism which allows them to obtain a decision and to execute this decision (7.1). As a private justice system, BDR must be able to inspire confidence by producing decisions that are fair. Otherwise, it will not be chosen by the disputants. In other words, the legitimacy of BDR rests in its ability to deliver fair justice (7.2). While BDRS render "fair and just" decisions with regard to the crypto-economic context, it is doubtful that their decisions can be considered fair in the legal sense of the term. This is a major impediment to the possible off-chain enforcement of BDR decisions (7.3).

7.1 *Providing Effective Justice*

We have seen that ODRS have been used to resolve disputes resulting from online transactions.[231] These private justice systems are often the only practical means of asserting a claim resulting from an online transaction, for example in e-commerce. By providing a simple, fast and cheap way to resolve small-claim

230 See *supra* chapter 3.2.2.

231 See *supra* chapter 4.

disputes, ODRs offer access to justice when the traditional state justice system is unable to deal with disputes because of the cost of legal proceedings – especially in an international context – and the huge number of disputes. Access to justice is the strongest benefit of ODRs.[232] On the other hand, the greatest drawback of the majority of ODRs is their inability to render decisions that can be enforced by state authorities or, failing that, are self-enforceable. An ODR mechanism that does not produce an enforceable outcome cannot provide effective access to justice.[233] The right to access to justice as stated in Article 6 para. 1 of the European Convention on Human Rights (ECHR) also encompasses the right to obtain the execution of judicial decisions.[234] The same applies to ODRs: effective access to justice implies that the outcome of ODR shall be enforceable. This is a central element for a justice system to inspire the confidence of its users.[235] E-commerce has shown that the ability of the justice system to inspire user confidence affects the entire environment it regulates.[236] When stakeholders have access to a trustworthy justice system, it strengthens their confidence in the business environment and benefits its development.

The experience with e-commerce can serve as a model for the crypto economy. If it truly wants to become a trustworthy business environment that fosters international transactions, the blockchain environment must incorporate a justice system that inspires user confidence. Granting effective access to justice to DAOs and other on-chain actors wishing to remain pseudonymous is essential to the future development of the crypto economy. To achieve this objective, BDRs must be able not only to render decisions, but also to enforce their own decisions. We have seen that BDRs have the power to directly and automatically enforce their own decisions on the blockchain through the use of smart contracts.[237] As the immutability of the system makes it impossible to rely on the intervention of outside actors or state enforcement authorities to execute by force a blockchain operation, the ability of BDR to be self-reliant

232 Same opinion: Loebl (n 169), 16.

233 See *e.g.*, Ruha Devanesan and Jeffrey Aresty, "ODR and Justice – An evaluation of Online Dispute Resolution's Interplay with Traditional Theories of Justice," in Mohamed S. Abdel Wahab, Ethan Katsh and Daniel Rainey (eds), *Online Dispute Resolution: Theory and Practice* (eleven 2012), 251, 269.

234 European Court of Human Rights, "Guide on Article 6 of the European Convention on Human Rights" (30 April 2021), para. 187, available at <https://www.echr.coe.int/documents/guide_art_6_eng.pdf> accessed 28 June 2023.

235 Same opinion: Koulu (n 169), 8; Loebl (n 169), 21.

236 See Katsh and Rabinovich-Einy (n 160), 73–75.

237 See *supra* chapter 5.3.

in the enforcement of its own decisions is crucial. This capacity offers a significant improvement over ODRs that do not use blockchain technology.

We have highlighted above[238] the four major issues arising in connection with disputes involving DAOs and preventing them from being resolved in state courts, which are the following: first, the localisation of operations that take place only on-chain within the borders of a specific state by using a connecting factor is most of the time impossible. Second, an entity without legal capacity cannot sue or be sued in its own name. Third, a lawsuit cannot be filed against a person whose identity and address is unknown. Fourth, enforcement of a decision by force, when the losing party does not comply voluntarily, is virtually impossible when enforcement involves the transfer of cryptocurrencies and other crypto assets or the performance of any other action on the blockchain. These four elements do not pose any particular problem when a dispute of a contractual nature involving a DAO or related to the governance of a DAO is resolved through BDR.[239] The role of BDRs is crucial for the balance of the crypto economy as they allow for the resolution of disputes that could not be effectively resolved by state courts. When on-chain actors are involved in relationships on the blockchain, BDRs prevent them from being denied justice. BDRs are therefore of paramount importance, considering that most of the activity in the crypto environment involves on-chain actors, such as maverick DAOs, who do not have access to justice outside of the blockchain. BDRs give the necessary stability to the crypto economy by bringing the hand of justice into this global business environment.

In comparison with state justice systems, the main drawback of BDRs is that they do not provide predictability as to the outcome of a dispute since jurors do not refer to a defined framework of rules or norms to make a decision, nor is the dispute resolution system based on precedent. The same situation can thus be solved differently depending on internal fairness considerations of each juror.[240] At the present stage of development, BDRs do not provide the same level of certainty as state courts, which apply rules of law. As a result, on-chain dispute resolution systems are not yet able to reduce the risk of litigation, which means that the costs associated with the risk of litigation must be taken into account when parties enter into a contractual relationship using a smart contract of a certain complexity that falls under the jurisdiction of a BDR mechanism. If BDRs are to be viable in the long term, they must find a configuration that ensures a certain level of predictability and therefore certainty

238 See *supra* chapter 3.
239 See *supra* chapter 6.
240 Buchwald (n 203), 1407.

in their decisions. Only then will they be a realistic option to overcome the legal uncertainty related to state justice, associated in particular to the difficulty to locate relationships performed on the blockchain. That said, it must also be recognised that if a dispute involving a DAO were to be submitted to the jurisdiction of state courts, it is very likely that the solution on the merits would differ from one state to another. The legal rules applicable to blockchain transactions are indeed still very disparate.[241] Legal diversity also brings legal uncertainty, maybe even more than a binary justice system where jurors must choose between two given solutions.

The main challenge for BDRs in providing effective justice is to find a way to resolve all types of disputes that might involve DAOs and to be able to enforce all their decisions. In their current state of development, an opt-in clause, encoded in one of the smart contracts governing the relationship between the parties, is necessary to subject disputes to the jurisdiction of a BDR mechanism.[242] If we get out of the contractual field or the governance of DAOs and venture into tort cases, an opt-in BDR is of no use as it would have no means to enforce a decision except if the defendant accepts to put assets within the power of the BDR mechanism.

In The DAO case, for example, BDR could have been used to settle the dispute among the members of The DAO who wanted to prove the hacker right and those who wanted to undo the effects of the hacking.[243] At that time, there was no BDR mechanism in operation and the dispute could only be resolved at the level of the underlying blockchain (*i.e.*, Ethereum). Since a great amount of circulating ethers were invested in The DAO, confidence in the network was greatly diminished. The hack was affecting the very existence of the Ethereum blockchain. This pushed a majority of members of the Ethereum community to agree to a hard fork[244] to reverse the hacker's misappropriation of The DAO's funds, which was very controversial. But a minority of members believed that the state of the blockchain should not be altered because blockchains are supposed to be immutable, and they considered that the hacker had simply used the code to its advantage. The dispute between both sides resulted in two

241 See Matthias Lehmann, "National Blockchain Laws as a Threat to Capital Markets Integration" (2021) 26 Uniform Law Review 148, for an analysis of French, English and American blockchain legislations.

242 See *supra* chapter 5.4.

243 See *supra* chapter 2.1.

244 See Koulu and Markkanen (n 82), 390–393; Werbach and Cornell (n 83), 351. For more information on soft and hard forks, see *e.g.*, "Soft fork vs. hard fork: Differences explained" (*Cointelegraph*) <https://cointelegraph.com/blockchain-for-beginners/soft-fork-vs-hard-fork-differences-explained> accessed 28 June 2023.

Ethereum blockchains being maintained: Ethereum classic, where the hacker's transactions were upheld, and Ethereum, where the hacker's transactions were deregistered. While both blockchains are functioning to date and both of their cryptocurrencies hold market value, a majority of the nodes have only been maintaining the Ethereum blockchain and have left Ethereum classic. This case shows that blockchains themselves can also be subject to disputes, just like any decentralised entity.[245] The community of a blockchain can disagree on what the state of the ledger should be. In The DAO case, the Ethereum community made the decision to modify the blockchain protocol to regulate the activities taking place on the network by invoking social norms.[246] This highlights the power of the community to exert direct influence on the state of the blockchain.

Even if a BDR mechanism had existed at the time of The DAO case, the solution would not necessarily have been different. The only way resorting to BDR would have been useful for the members of The DAO who had their investment defrauded is if the hacker had agreed to place the stolen ethers under the jurisdiction of the BDR mechanism, which is highly unlikely. Otherwise, the BDR mechanism's decision would have been only symbolic and effective justice could not have been provided. However, in such disputes involving a tort, other mechanisms could be imaged to allow BDRs to indirectly enforce their decisions without having power over the disputed cryptocurrencies or crypto assets. For example, a BDR mechanism could allow the victim of a wrongful act on the blockchain (*e.g.*, a hack) to unilaterally seize its court. The claim would be made public and the BDR mechanism would invite the perpetrator to defend itself. In the event that a decision finding the perpetrator guilty is rendered and the perpetrator refuses to compensate the victim for the damage, the BDR mechanism could place the perpetrator (*i.e.*, the wallet address where the disputed crypto assets are located) on a blacklist. The legitimacy of such a decision would likely be recognised by the entire community because a decision rendered by BDR is one rendered by a jury of peers representing the community. The enforcement of the decision of the BDR mechanism would be indirectly performed by the actors of the crypto economy who refuse to enter into business relations with a blacklisted user. Compliance with social norms would thus be the basis for the enforcement of the BDR decision by each member of the community. The role of a BDR mechanism as a court could even be pushed to the next level: instead of being an opt-in dispute resolution

245 Some blockchains, such as Bitcoin and Ethereum, can be characterised as DAOs. See *supra* n 17.

246 De Filippi and Wright (n 13), 188–189.

mechanism, a BDR mechanism could be implemented into a blockchain's core protocol so that it would be granted jurisdiction over all transactions within this blockchain.

7.2 *Providing a Fair Resolution of Disputes*

BDRs make the most of blockchain technology by producing outcomes that are directly and automatically enforceable by the computer system. But this is not enough to bring truly effective justice in the crypto economy. In order to acquire legitimacy, a BDR mechanism must inspire confidence from the actors of the blockchain ecosystem in its dispute resolution mechanism. This confidence in the justice system is crucial for building trust in the blockchain-based economic environment. Confidence in a BDR mechanism – and thus its legitimacy – is associated with its ability to render fair decisions. But are BDR decisions fair? It is not possible to answer this question in a binary way by choosing between the option "the decisions of a BDR mechanism are fair" and the option "the decisions of a BDR mechanism are not fair." The answer depends not only on each case examined, but especially on the respondent's frame of reference. The resolution of a dispute can be fair without being legally fair. A conflict resolution system must be configured to match the expectations of its users. While a state justice system is expected to be fair in the legal sense (7.2.1), a private justice system may depart from this model to fit the socio-economic environment it is called upon to regulate (7.2.2).

7.2.1 Fair Justice in the Legal Sense

So, are BDR decisions fair? A lawyer would likely answer "no." BDR jurors are anonymous and buy their way into office. As such, they have a direct economic interest in the outcome, which leads them to disregard the solution that seems fair based on an assessment of the facts and an application of the law, and to opt instead for the decision that is most likely to be chosen by the other jurors. In those conditions where economic interests are prominent, a BDR decision cannot be fair in the legal sense of the term. This type of decision offends the sense of justice as defined in legal instruments aimed at protecting the fundamental procedural rights of the parties to proceeding. It is universally accepted that every person has the right to have its case heard by a competent, independent, and impartial tribunal as defined under Article 6 para. 1 of the ECHR, Article 14 para. 1 of the International Covenant on Civil and Political Rights (ICCPR), and Articles 8 and 10 of the Universal Declaration of Human Rights (UDHR).

The obligation of ODRs to respect fundamental procedural rights has been recalled on several occasions at the supra-national level.[247] In its Technical Notes on Online Dispute Resolution, UNCITRAL made it clear how important it is that ODRs respect the "principles of impartiality, independence, efficiency, effectiveness, due process, fairness, accountability and transparency."[248] The United Nations Conference on Trade and Development (UNCTAD) referred to the same basic quality criteria for the evaluation of ODRs dealing with e-commerce disputes.[249] This reflects the concern of the international community that ODRs provide a justice system that guarantees respect for fundamental rights even if they are not part of the state justice system. Among legal scholars, there is a consensus that procedural minimum standards must be applicable to ODRs, even in the absence of unified rules of procedure adopted at a supra-state level.[250] Justice achieved through an ODR mechanism can only be effective if procedural minimum standards are respected. ODRs are encouraged to spontaneously comply with minimum standards as to the technological and legal requirements, since there is no global supra-state body with the necessary authority to verify their effective compliance.[251]

---

247 See *e.g.*, Organization for Economic Cooperation and Development (OECD), "The Economic and Social Role of Internet Intermediaries," April 2010 <https://www.oecd.org/internet/ieconomy/44949023.pdf> accessed 28 June 2023. In the EU, see *e.g.*, Council of Europe, Recommendation CM/Rec(2018)2 of the Committee of Ministers to Member States on the roles and responsibilities of internet intermediaries, 7 March 2018; European Parliament, Digital Services Act: Opportunities and Challenges for the Digital Single Market and Consumer Protection, Collection of Studies for the IMCO Committee, June 2020 <https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/652712/IPOL_BRI(2020)652712_EN.pdf> accessed 28 June 2023.

248 UNCITRAL (n 184), para. 4.

249 UNCTAD, "Dispute resolution and redress," 30 April 2018, TD/B/C.I/CPLP/11, para. 43.

250 See *e.g.*, Loebl (n 169); Richard Susskind, *Online Courts and the Future of Justice* (Oxford University Press 2019); Wang (n 162); Leah Wing, "Ethical Principles for Online Dispute Resolution – A GPS Device for the Field" (2016) 3 International Journal on Online Dispute Resolution 1; Devanesan and Aresty (n 233), 263–292; Lodder and Zeleznikow (n 189), 18–38; Kaufmann-Kohler and Schultz (n 157), 108–119.

251 However, there is an accreditation system for ODR providers in the EU under which they must comply with minimum standards. See Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) N 2006/2004 and Directive 2009/22/EC (Directive on Consumer ADR), [2013] OJ L 165/63, and Regulation (EU) N 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes and amending Regulation (EC) N 2006/2004 and Directive 2009/22/EC (Regulation on Consumer ODR), [2013] OJ L 165/1.

In this legal conception of the fairness of justice, decisions rendered by the BDRs that have been examined (*i.e.*, Kleros and Aragon Court) cannot be qualified as fair.[252] While it could be argued that those mechanisms respect due process to some degree because the parties can submit evidence, and that the jury is independent because each juror is chosen randomly,[253] the fact remains that jurors have an economic interest that is linked to the chosen solution, which pushes for the popular solution to be chosen rather than the fair one. That being said, major ODRs such as eBay's Money Back Guarantee depart much further from the fundamental rights mentioned above and the concept of fair justice in the legal sense. In eBay's model, the e-commerce platform has a corporate interest in the resolution of the conflict, which may skew its decisions. Some sellers have expressed their concern that eBay is the judge, the jury, and the executioner[254] and some others have reported that chargebacks have been unfairly executed to please the buyers.[255] It appears that eBay's ODR unfairly favours the buyer and does not provide the seller with sufficient recourse options.

7.2.2 Fair Justice in the Crypto-economic Sense

Economists, as well as actors of the crypto economy, will not necessarily refer to the legal sense of fair justice to assess the quality of decisions made by BDR. Lodder and Zeleznikow noted that an ODR mechanism which uses game-theoretic techniques to resolve a dispute is "fair in the sense that each disputant's desire is equally met. [It does] not, however, meet concerns about justice."[256] These authors highlighted that an ODR mechanism which uses principles of game theory for resolving disputes has the advantage of avoiding the parties negotiating "in the shadow of the law,"[257] which means taking into

252 See Robert J. Condlin, "Online Dispute Resolution: Stinky, Repugnant, or Drab" (2017) 18 Cardozo Journal of Conflict Resolution 717, 758. Other opinion: Daniel Dimov, "Crowdsourced Online Dispute Resolution" (thesis University of Leiden 2017), available at <https://ssrn.com/abstract=3003815> accessed 28 June 2023, who proposes a model of ODR procedure that complies with the procedural minimum standards. Kleros claims using a procedure consistent with this interpretation; see Ast and Deffains (n 195), 252–254.

253 See *supra* chapter 6.

254 See several posts on the eBay community page: https://community.ebay.com/ accessed 5 November 2021.

255 See "eBay sellers can no longer use PayPal under new terms" (*BBC News*, 1 June 2021) <https://www.bbc.com/news/technology-57318294> accessed 28 June 2023.

256 Lodder and Zeleznikow (n 189), 91.

257 In the words of Robert H. Mnookin and Lewis Kornhauser, "Bargaining in the Shadow of the Law: The Case of Divorce" (1979) 88 The Yale Law Journal 950. In ADR proceeding, the

account what would be possible to obtain in a judicial proceeding.[258] In BDR, the rules of the code prevail over the rules of law. This makes it possible to dispense with the concept of "legally just and fair" in favour of the concept of "just and fair" by avoiding, in particular, a juror being seen as biased by the solution that is legally valid.[259] Richard Susskind has come to the same conclusion by considering that the decision of an ODR mechanism must above all "reflect a popular sense of right and wrong."[260] The defendant's right to a fair trial could thus be guaranteed in ODR and BDR proceedings without necessarily complying with the wording of Article 6 para. 1 ECHR, Article 14 para. 1 ICCPR, and Articles 8 and 10 UDHR.[261]

Some authors have highlighted the fact that the particularities of the socio-economic environment of the Internet need to be considered to assess the concept of justice for online transactions.[262] A system of justice must above all be perceived as fair by the community using it. In other words, the expectations of the actors of the blockchain community are important to assess the fairness of the justice rendered by BDR.[263] Blockchain users think that this technology, which is fundamentally based on the use of cryptographic protocols and economic incentives, has the capacity to maintain confidence in social and economic relations.[264] It is therefore not surprising that a BDR mechanism should offer a conflict resolution mechanism based solely on "strict economic incentives achieved through mechanism design" and that jurors are expected to act honestly because "it is in their rational interest to act in such a way in order to optimise their economic gain."[265] In such a system of "decentralized justice,"[266] where fairness in the decision-making process is achieved primarily

---

parties usually bargain "in the shadow of the law," meaning that they do not apply the rules of law but are aware of their existence and their potential application.

258 Lodder and Zeleznikow (n 189), 165–166.

259 Buchwald (n 203), 1404–1408, has pointed out how problematic the lack of reference to a legal framework is in the long term.

260 Susskind (n 250), 76.

261 See Willemien Netjes and Arno R. Lodder, "e-Court – Dutch Alternative Online Resolution of Debt Collection Claims. A Violation of the Law or Blessing in Disguise?" (2019) 6 International Journal of Online Dispute Resolution 96.

262 See *e.g.*, Katsh and Rabinovich-Einy (n 160), 164–165.

263 Same opinion: Koulu and Markkanen (n 82), 397–399.

264 See Vitalik Buterin, "On Public and Private Blockchains" (*Ethereum blog*, 7 August 2015) <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/> accessed 28 June 2023. See also Jack Parkin, *Money Code Space – Hidden Power in Bitcoin, Blockchain, and Decentralisation* (Oxford University Press 2020), 20–23.

265 Ast and Deffains (n 195), 249–250.

266 The term "decentralized justice" is borrowed from Kleros, *Dispute Revolution – The Kleros Handbook of Decentralized Justice* (Kleros 2020), available at <https://kleros.io/book.pdf> accessed 28 June 2023.

through the use of crypto-economic mechanisms, it is clear that the notion of fair justice departs from that which prevails in state justice, where the focus is to protect the fundamental procedural rights of parties. The dispute resolution mechanisms used by Kleros and Aragon are indicative of a new approach to dispute resolution, devised by computer scientists and economists, in which the rules of law are replaced by the rules of the market, including reputation, speculative predictions, profit-seeking and trust.[267] This approach is consistent with the ideology behind the creation of a crypto economy independent of any state influence, in the sense that the law of the states should (or could) not apply in this "anational" environment.[268] De Filippi and Wright noted in this regard that "[a]s a general rule, because of their decentralized and transnational nature, blockchain-based systems exhibit a degree of *alegality*".[269]

Actors of the blockchain must have confidence in the dispute resolution mechanism for it to acquire legitimacy. Confidence in the dispute resolution mechanism is paramount in a private justice system that derives its legitimacy from the parties' choice to submit their dispute to its jurisdiction. As a private justice system, a BDR mechanism must be tailored to the expectations of the disputants in order for them to choose it. In relation with Kleros, it was noted that "[a]t the heart of dispute resolution lies the concept of legitimacy, which is ultimately premised on trust (trust in the system, trust in the process and trust in its fairness) and therefore a willingness to abide by outcomes."[270] Confidence is brought by fair decisions. This requires, among other things, that disputants feel that the decision-making process gives them the opportunity to make their case. The right to be heard is indeed essential to satisfy the subjective sense of justice.[271]

---

267 For a critical approach, see Matthew Dylag and Harrison Smith, "From cryptocurrencies to cryptocourts: blockchain and the financialization of dispute resolution platforms" (*Taylor & Francis Online*, 23 June 2021) <https://www.tandfonline.com/doi/full/10.1080/1369118X.2021.1942958> accessed 28 June 2023. For a global analysis of the legal challenges related to regulation by blockchain technology, see Paolo Tasca and Riccardo Piselli, "The Blockchain Paradox," in Philipp Hacker and others (eds), *Regulating Blockchain – Techno-Social and Legal Challenges* (2019 Oxford University Press), 27; Primavera De Filippi and Samer Hassan, "Blockchain technology as a regulatory technology: From code is law to law is code" (*First Monday*, 5 December 2016) <https://firstmonday.org/ojs/index.php/fm/article/view/7113/5657> accessed 28 June 2023.

268 Guillaume (n 1), 183–184.

269 De Filippi and Wright (n 13), 44.

270 Ast and Deffains (n 195), 243.

271 See Koulu and Markkanen (n 82), 398; Fahimeh Abedi, John Zeleznikow and Emilia Bellucci, "Universal standards for the concept of trust in online dispute resolution systems in e-commerce disputes" (2019) 27 International Journal of Law and Information

With the exception of classic arbitration, private justice systems do not need to respect fundamental rights of the parties as a state court does. But the higher the stakes of the disputes submitted to BDR, the more the dispute resolution mechanism should take into account moral, social and political norms.[272] If a BDR mechanism is chosen to resolve disputes that affect people's lives as individuals, the decisions it renders could have a much more profound impact than minor disputes arising from a simple contractual relationship, which can only lead to economic effects of marginal significance. The expectations of the parties as to the fairness of the decision are higher in this type of case. This is the reason why the justice system defined by the BDR mechanism's code must then be "reasonable, caring and fair"[273] in order to produce decisions that are just and fair.[274] As Lessig has demonstrated, the code can reflect such values since it is not value neutral.[275] However, as long as the complexities of judicial procedures cannot be reduced to a set of mathematical axioms, the decision-making process of a BDR mechanism will not be as fair in the legal sense as decisions from traditional courts.[276] In reality, disputes that can be resolved by a binary "if/then" equation are a very small part of commercial and private life.

The model followed by existing BDRs is a departure from the jury model used in state courts and is closer to the arbitral tribunal model. In the dispute resolution model adopted by Kleros and Aragon Court, jurors are anonymous (or pseudonymous), and cannot communicate with each other, which has the effect that each juror makes an individual decision without consulting the other jurors. The decision resulting from this process is a popular decision that reflects a form of consensus because it corresponds to a universality of opinions for the purpose of reaching the wisdom of the crowd. However, one can

---

Technology 209, 226; Anjanette H. Raymond and Scott Shackelford, "Technology, Ethics, and Access to Justice: Should an Algorithm be Deciding Your Case?" (2014) 35 Michigan Journal of International Law 485, 516–519; Rebecca Hollander-Blumoff and Tom R. Tyler, "Procedural Justice and the Rule of Law: Fostering Legitimacy in Alternative Dispute Resolution" (2011) Journal of Dispute Resolution, available at <https://scholarship.law.missouri.edu/cgi/viewcontent.cgi?article=1612&context=jdr> accessed 28 June 2023.

272 About the consideration of moral, social and political norms in the dispute resolution system, see Condlin (n 252), 733–734.

273 Condlin (n 252), 734.

274 However, the rules incorporated in the code of a smart contract are not (yet) able to achieve this goal because they are less flexible than the rules of law. Several authors speak in this respect of the "tyranny of code". See Perritt (n 137), 225; De Filippi and Wright (n 13), 205–210.

275 Lawrence Lessig, *Code. Version 2.0* (Basic Books 2006), 124–125.

276 Same opinion: Dylag and Smith (n 267); Buchwald (n 203).

wonder whether a sum of individual decisions rather than a collective opinion can lead to a just and fair decision. Especially considering that jurors are driven by economic incentives not to decide according to what they think is the right answer but what they think the popular opinion will be. Furthermore, the jury is often composed of too few people to be considered representative of the community. This is compounded by the fact that, unlike arbitrators, jurors are not selected primarily on the basis of their qualifications but on their economic contribution in the system, creating a significant risk that the power of justice will be in the hands of a very small number of community members who also hold the financial power.[277] The crypto-economic model adopted by existing BDRs still needs to be improved in order to be sufficiently just and fair to be entrusted with resolving disputes that are not entirely economic in nature but may impact individuals' personhood.

7.3 *Issue of the Off-Chain Effect of a BDR Decision*

From the point of view of economists and computer scientists, BDR is able to guarantee effective and fair access to justice without necessarily complying with minimum procedural guarantees as high as those required from state courts in the vast majority of countries. The dispute resolution mechanisms implemented in the two BDRs we studied provide effective justice not only by producing decisions that are directly and automatically executed by the system, but are also viewed as fair by the actors of the crypto economy. They have the double benefit of matching the expectations and needs of the actors of the crypto economy and of being adapted to the particularities of the crypto-economic system. They are therefore likely to inspire user confidence and to be accepted by the actors of the crypto economy.[278] We are thus in the presence of an actual justice system specific to the crypto economy which is independent and autonomous from the states.

While a key element of any justice system is its ability to enforce the decisions it produces, we have seen that the dispute resolution system implemented by BDRs, such as Kleros and Aragon Court, is limited in scope to cryptocurrencies and other crypto assets, as well as actions that can be put within their power by means of a smart contract (the so-called "statutory deposit").[279] However,

277 See also Dylag and Smith (n 267), who state that the administration of justice is placed in the hands of a "technocratic elite."

278 See World Economic Forum (WEF), "Bridging the Governance Gap: Dispute Resolution for Blockchain-Based Transactions," 16 December 2020, 6 <https://www.weforum.org/whitepapers/93bd1530-0ded-48fa-8dee-e9b2d109d84d> accessed 28 June 2023.

279 See *supra* chapter 5.3.

a dispute involving a DAO may also concern non-crypto assets or actions that need to be performed outside the blockchain. In this case, the decision arising from a BDR mechanism cannot be directly and automatically executed through a smart contract. Therefore, the intervention of state authorities may be required to enforce the decision in the physical world. This raises the question of recognition and enforcement of a decision arising from a BDR mechanism in a state jurisdiction for its execution on non-crypto assets with the assistance of state authorities. Such an operation is only possible if the legitimacy of the dispute resolution mechanism offered by BDR is recognised by the states. If this is not the case, the effectiveness of the BDR justice system would be limited to the crypto environment.

Should a BDR decision be enforced off-chain, respect for the procedural fundamental rights of the parties will in principle be verified at the time of enforcement by state authorities. Enforcement outside the blockchain environment (*e.g.*, execution on non-crypto valuable resources) will not be possible if the decision cannot be qualified as fair in the legal sense. Indeed, the decision will not be recognised and enforced by state authorities if it is manifestly incompatible with the public policy of the requested state. The concept of *ordre public* aims to protect in particular the fundamental principles of procedural fairness. This could be an issue when a decision made by a BDR mechanism cannot be executed entirely on-chain and has to be executed in part or entirely off-chain.

The ability to enforce off-chain a decision rendered by a BDR mechanism depends on the rules that are applicable in the state in which enforcement is being sought. The authors are not aware of any decisions made by Kleros or Aragon Court that have already been enforced as such by state authorities. It is interesting to examine in this respect two different situations: first, the application of the New York Convention (7.3.1) and second, the application of a PIL convention allowing the recognition or enforcement of a foreign judgment (7.3.2).

7.3.1 Off-chain Enforceability of a BDR Decision as an Arbitral Award?

In the opinion of the authors, the decisions of the BDRs that have been studied in this article are made in the context of non-binding arbitration proceedings.[280] This follows, among other things, from the fact that a BDR decision is, by definition, not made in the territory of a state. The decentralisation characteristic

280 See *supra* chapter 4.1.2.

of this private justice system means that there is no seat of arbitration.[281] It is therefore not possible to formally attribute the enforceability or *res judicata* effect of a BDR decision to the law of a state. As such, the decisions made by those BDRS are not enforceable by state authorities in the same manner as judgments rendered by state courts as opposed to arbitral awards rendered in classic arbitration.

The term "BDR" as defined by the authors[282] only covers dispute resolution mechanisms that exclusively use blockchain technology to provide and enforce decisions. BDRS offer an on-chain-only dispute resolution mechanism. ODRS that offer the services of arbitrators who render arbitral awards using blockchain technology is outside the research field of this paper. When an arbitrator issues an arbitral award by somehow using the services of a blockchain-based ODR mechanism, it is quite conceivable that the ensuing arbitral award can be enforced under the New York Convention. For example, when an arbitrator acts as an interface between a BDR mechanism (*e.g.*, Kleros) and a state jurisdiction, the BDR decision can be transcribed into an arbitral award that meets the requirements of formal and substantive validity in order to be recognised and enforced by state authorities. This situation arose in a case where the parties to a real estate leasing agreement over a property located in the state of Jalisco, Mexico, agreed to have a sole arbitrator resolve their dispute in connection with that agreement using Kleros to render the decision. The arbitrator instrumented the proceedings, submitted the case to Kleros and "formalised" Kleros's decision (rendered unanimously by three anonymous jurors on 23 November 2020) by transcribing it into an arbitral award that met the formal and substantive validity requirements of the state of Jalisco. The arbitral award was subsequently enforced by the Mexican authorities. However, the application of the New York Convention was not needed in this particular case, as it was a domestic arbitration governed by Mexican procedural law.[283] This

281 Same opinion: Maxime Chevalier, "From Smart Contract Litigation to Blockchain Arbitration, a New Decentralized Approach Leading Towards the Blockchain Arbitral Order" (2021) Journal of International Dispute Settlement 1, 12.

282 See *supra* chapter 5.1.

283 This Mexican case is described in detail by the arbitrator: Mauricio Virues Carrera, "Accommodating Kleros as a Decentralised Dispute Resolution Tool for Civil Justice Systems: Theoretical Model and Case of Application" (with the documents of the procedure attached), available at <https://ipfs.kleros.io/ipfs/QmfNrgSVE9bb17KzEVFoGf4KKA1Ekaht7ioLjYzheZ6prE/Accommodating%20Kleros%20as%20a%20Decentralized%20Dispute%20Resolution%20Tool%20for%20Civil%20Justice%20Systems%20-%20Theoretical%20Model%20and%20Case%20of%20Application%20-%20Mauricio%20Virues%20-%20Kleros%20Fellowship%20of%20Justice.pdf> accessed 5 November 2021.

very unusual situation (for the time being) is beyond the scope of this study because Kleros was used as a mere tool in the decision-making process of an arbitrator acting in the context of arbitral proceedings.

If we were to consider that a BDR decision was rendered in the context of international arbitration proceedings, the decision would have to be analysed in light of the New York Convention in order to determine whether it could be recognised and enforced in a contracting state. The New York Convention provides several grounds for refusing to recognise or enforce an arbitral award in its Article V. In the opinion of the authors, a BDR decision does not in any case fall within the scope of application of this instrument. Nevertheless, and for the sake of the argument, the main grounds that could pose a problem when the enforcement of a decision rendered by a BDR mechanism is requested in application of the New York Convention will be listed, without going into the details of its Article V.[284]

First, a decision is not enforced if the arbitral agreement is invalid. This covers, in particular, incapacity of the parties. The validity of the arbitral agreement could thus be called into question, at the stage of enforcement of the decision, when one of the parties does not have the capacity to make a legally valid commitment (*e.g.*, a maverick DAO). Furthermore, it is not certain that an arbitral agreement concluded by electronic means (*e.g.*, by smart contract) meets the requirements of formal validity.[285] This question may be answered differently depending on the state in which enforcement is sought.

Second, enforcement may be refused if the scope of the decision goes beyond what is agreed in the arbitral agreement. To the extent that the scope of a BDR mechanism is limited, as it stands, to the valuable resources within its jurisdictional power,[286] the off-chain enforcement of the decision could be challenged in the absence of an agreement by the parties on this issue.

Third, enforcement of an arbitral award may be refused if it has not yet become binding on the parties. In the opinion of the authors, the decisions rendered by BDR are not binding on the parties since they have not acquired enforceability or *res judicata* effect under the law of a state. However, the

284 It should be noted that some blockchain-based ODR projects intend to use blockchain technology only for the decision-making process, but do not take advantage of its execution potential. Those projects are trying to set up systems whereby they could render decisions that could be qualified as arbitral awards in order to take advantage of the enforcement system of the New York Convention. One famous example is the project Decentralized Arbitration and Mediation Network (DAMN) proposed in early 2016 to The DAO community, but which was never achieved because of the early fall of The DAO.

285 Same opinion: Chevalier (n 281), 14–15.

286 See *supra* chapter 5.3.

question of whether a BDR decision is "binding on the parties" within the meaning of the New York Convention may be answered differently from state to state.

Fourth, the enforcement can be refused on public policy grounds, which is the most important safeguard. There is no doubt that the lack of legal fairness would be raised in the event that a party attempts to obtain the off-chain enforcement of a BDR decision. It would then be up to the recognition authority in the requested state to determine whether or not recognition of the BDR decision is contrary to the public policy of its state.

This brief analysis shows that the application of the New York Convention to a decision rendered by a BDR mechanism – and more generally to decisions rendered by an ODR mechanism[287] – raises many questions that have not yet been clearly answered. The possibility that some states will agree in the future to recognise and enforce BDR decisions under the New York Convention cannot be excluded. It is nevertheless dubious that such decisions could be enforced in all the contracting states of the New York Convention. Furthermore, some states may agree to enforce the decisions rendered by BDRs under their national rules of PIL or their domestic rules of procedural law. But this would at least require that BDR decisions be characterised as arbitral awards and be compatible with the public policy of the state in which enforcement is sought.

7.3.2 Off-chain Enforceability of a BDR Decision as a Foreign Judgment?

Since it is very unlikely that a BDR decision could be recognised or enforced as an arbitral award under the New York Convention, the question arises as to whether it could be recognised as a foreign judgment under a PIL convention allowing the recognition or enforcement of foreign judgments. For the sake of the argument, three international instruments deserve to be examined in this context, even if a BDR decision is not enforceable in the same manner as a judgment in the opinion of the authors.

The Hague Convention on the Recognition and Enforcement of Foreign Judgments of 2 July 2019 (the "Judgments Convention") is the first international instrument worthy of consideration. However, a BDR decision does not qualify as a "judgment" within the meaning of the Judgments Convention, because it is not a "decision on the merits given by a court."[288] The term "court" is not

287 See *e.g.*, Mohamed S. Abdel Wahab, "ODR and E-Arbitration – Trends and Challenges," in Mohamed S. Abdel Wahab, Ethan Katsh and Daniel Rainey (eds), *Online Dispute Resolution: Theory and Practice* (eleven 2012), 387, 392–395.

288 See Art. 3 para. 1 sub-para. b of the Judgments Convention.

defined in the Convention, but there is a consensus that this word does not refer to "non-state authorities."[289] The application of this convention is therefore irrelevant.[290]

The Hague Convention on choice of court agreements of 30 June 2005 (the "Choice of Court Convention") could be applicable to the recognition or enforcement of a BDR decision. This Convention facilitates the recognition and enforcement of a judgment given by a court of a contracting state designated in an exclusive choice-of-court agreement in another contracting state. Entrusting the resolution of a dispute to BDR necessarily results from an agreement between the parties (an opt-in clause), which could possibly be assimilated to a choice-of-court clause.[291] However, the scope of application of the Choice of Court Convention is the same as the one of the Judgments Convention regarding the concept of "judgment."[292] The rules of recognition and enforcement contained in this convention are therefore only applicable to decisions rendered by a state authority. Thus, to this day, the Choice of Court Convention cannot apply to the recognition and enforcement of outcomes of the two BDRs that have been studied for this paper.

The Lugano Convention could be applied if a BDR decision could be qualified as a judgment within the meaning of "any judgment given by a court or tribunal of a state bound by [the] Convention."[293] In the opinion of the authors, this is not the case and the Lugano Convention cannot be applied to recognise or enforce a BDR decision either.

The fact that these three international instruments apply only to the recognition or enforcement of judgments rendered in another contracting state is a strong impediment to their application to decisions rendered by BDRs since these can neither be attached to a state authority nor to the territory of a contracting state. Furthermore, what has just been said about the New York Convention[294] is also valid for the two Hague Conventions as well as the Lugano Convention: the grounds for refusal of recognition or enforcement of all these instruments have almost all the same effect. Compatibility of the decision with the public policy of the requested state is a *sine qua non* condition

289 See Francisco Garcimartin and Geneviève Saumier, *Explanatory Report of the Convention of 2 July 2019 on the Recognition and Enforcement of Foreign Judgments in Civil or Commercial Matters* (HCCH 2020), para. 101–102.

290 Furthermore, the Judgments Convention does not apply to arbitration according to its Art. 2 para. 3.

291 See *supra* chapter 5.4.

292 Art. 4 para. 1 of the Choice of Court Convention.

293 Art. 32 of the Lugano Convention.

294 See *supra* chapter 7.3.1.

for the enforcement of the decision. Both Hague Conventions expressly state that the enforcement of a decision is refused in "situations where the specific proceedings leading to the judgment were incompatible with fundamental principles of procedural fairness of that State."[295] This is also valid, *mutatis mutandis*, when the Lugano Convention applies.

Without an international instrument that could be applicable to the enforcement of a decision rendered by a BDR mechanism, such a decision could only be enforced in a state if its national rules of PIL allow it. This presupposes that the requested state agrees to give effect to a BDR decision in its territory by enforcing it as if it were a foreign judgment. However, this seems even more doubtful than the enforcement under the rules applicable to arbitral awards.

It must be concluded that the off-chain enforcement of BDR decisions is unlikely in the current state of development of BDRs. When the decision arising from a BDR mechanism is to be enforced on non-crypto assets and cannot be recognised or enforced in the state where the enforcement is to take place, the BDR justice system loses its effectiveness. If the losing party does not voluntarily comply with the decision, the other party must accept that the dispute should be (re)submitted to a judge who will render a judgment on the basis of their assessment of the facts as well as the legal situation. Nevertheless, it is up to each state to determine whether, in the future, it is prepared to enforce decisions that do not respect fundamental procedural rights. One can assume that BDRs will have to implement justice systems governed by their code that better respect the fundamental procedural rights of the parties for their decisions to be recognisable or enforceable in state jurisdictions. For the time being, it is premature to count on the recognition of the legitimacy of the BDR justice system by states. In any case, the two systems of justice do not need to be interconnected for BDRs to deliver effective and fair justice in the crypto environment.

8 Conclusion: BDRs are Decentralized Autonomous Justice (DAJ)

The deployment of Bitcoin in 2008 has greatly impacted the ways in which communities of peers can come together and organise their activities in an independent and autonomous way. Satoshi Nakamoto laid out the first stone

295 Art. 7 para. 1 sub-para. c of the Judgments Convention; Art. 9 sub-para. e of the Choice of Court Convention.

with a peer-to-peer electronic cash system[296] that would enable millions of people around the globe to access money in a more democratic way and eliminate the need for intermediaries. Then, Ethereum has allowed users to build more complex systems on the same peer-to-peer architecture that made Bitcoin so unique. DAOs are now reinventing the way people can contract and organise, which is generating a whole new economy led by DeFi. DAOs are also giving rise to other novelties such as decentralised identity, which is promising to restructure the currently physical and digital identity ecosystem into a decentralised and democratised architecture. With decentralised governance and autonomy from central institutions, DAOs represent a new type of democratically run economic and social entities which promise to be fairer and to benefit all the members of their communities.

As with any social environment, the blockchain ecosystem rapidly saw the need for dispute resolution mechanisms to be available to DAOs and other actors of the blockchain economy. Traditional state justice was not the answer because of the autonomy of blockchain technology. A similar phenomenon was seen with the rise of the Internet and e-commerce, when a plethora of ODRs were developed for new kinds of disputes that were unsuitable for state courts. Small-claim disputes between people from different jurisdictions led Internet actors such as eBay to develop dispute resolution mechanisms that are specifically designed to meet the needs of their e-commerce platform: render high-volume enforceable decisions in a cheap and quick way. However, this model of ODR remains dependent on payment service providers that can charge additional fees, and often decisions are made unilaterally and can seem arbitrary.

BDRs such as Kleros and Aragon Court answer the needs of their own ecosystem by providing DAOs and other actors of the crypto economy with dispute resolution mechanisms that can render enforceable decisions in a cheap and quick way. While pseudonymity and lack of legal capacity prevent those actors from seeking justice in state courts, they are not obstacles to delivering justice in the blockchain environment. The only limits to BDR's power of enforcement are technological constraints. Whether a dispute is of a contractual nature or pertains to the governance of a DAO, smart contracts allow BDRs to render decisions and directly enforce them so long as valuable resources are in their technological environment. Kleros and Aragon Court have created independent and self-reliant justice systems that function without the intervention of state authorities or other intermediaries at any point in either the

296 Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 6, available at <https://bitcoin.org/bitcoin.pdf> accessed 28 June 2023.

decision-making process or the execution of the decision. Furthermore, as they run on blockchains and are themselves organised as DAOs, BDRs are autonomous systems that are shielded against any outside authority. In particular, states do not have the power to interfere with the decision-making process and the enforcement of a BDR decision. As such, BDRs are not only independent, but also autonomous.

Along with their independence and autonomy, BDRs have a monopoly of justice within the crypto environment. Even though the kind of justice they offer does not meet procedural standards set by states and cannot be qualified as fair justice in the legal sense, BDRs nonetheless offer a kind of justice that is fair in the crypto-economic sense. But most importantly, it is an effective justice in that the parties are provided with directly enforced decisions. This has been enough for the actors of the crypto environment to have confidence in this justice system as it is one that portrays the crypto-economic mechanisms which are the underlying foundations of the blockchain ecosystem. Actors who wish to submit to BDR can obtain a decision which first of all is rendered by their peers through mechanisms that use game theory and economic incentives and secondly is automatically enforced by the smart contract.

BDRs do not need to render decisions that can be recognised by states as arbitral awards or as foreign judgements to uphold their legitimacy, as long as the decisions they render are fully executed on-chain. Individuals make the deliberate decision to submit to BDRs for their on-chain activities, and BDRs offer a system of justice that matches the moral, social, and political ideals of the crypto environment. When individuals choose a service offered in the blockchain environment by an independent and autonomous platform (*e.g.*, DeFi services provider, decentralised identity provider, *etc.*) over its counterpart offered by traditional institutions (*e.g.*, banks, governmental agencies, *etc.*), it is only legitimate that the chosen Decentralized Autonomous Justice (DAJ) system rules over disputes that occur on that platform.

There is already a long tradition of submitting international commercial disputes to ADRs such as arbitration, and the BDRs we have analysed created a new milestone by bringing decentralisation and autonomy to private justice. However, the crypto environment is already developing towards much more personal matters that state jurisdictions have traditionally kept within their power to safeguard public policy interests. For example, a Proof of Humanity dApp is inviting individuals to prove their "humanity" (*i.e.*, the fact that they are an actual person) so that they be awarded a daily crypto income.[297]

297 See <https://www.proofofhumanity.id> accessed 28 June 2023.

Members of the community can challenge the alleged humanity of a user and Kleros has jurisdiction over determining whether an applicant is an actual human and qualifies for the unconditional basic income. It is undeniable that people around the globe are starting to entrust on-chain self-sovereign institutions with matters that affect their personhood, and this trust is reinforced by access to a DAJ system. Those individuals are no longer part of simple on-chain communities; they belong to a fully-fledged crypto jurisdiction.

CHAPTER 21

Recognition and Enforcement of the Outcome of Blockchain-Based Dispute Resolution

Pietro Ortolani

1 Introduction

Over the past decade, "blockchain" has become a buzzword. Proposals for the use of blockchain technologies abound in many fields, and the proliferation of vaguely worded "white papers" makes it often difficult to distinguish the facts from the "hype." Dispute resolution is no exception: numerous attempts are currently being made to develop blockchain-based procedures, which are supposed to deliver fast, reliable and tamper-resistant resolution of disputes. This chapter investigates whether the outcomes of these procedures may be recognised and enforced and, if so, under which legal regime. The analysis will refer to several of the currently existing blockchain-based dispute resolution procedures. However, considering the fast pace at which the technological landscape evolves, an attempt will be made to draw legal conclusions which can be applied in a more general fashion, rather than with exclusive regard to any particular blockchain-based procedure currently existing on the market. Furthermore, some sections of the chapter will look at the future, and consider some blockchain applications which have been proposed and theorised, but do not yet exist.

The chapter proceeds as follows. Section 2 provides a descriptive overview of the different attempts that have been made to date to develop blockchain-based dispute resolution mechanisms. Section 3, in turn, discusses the legal qualification of these mechanisms, analysing in particular under which conditions they may qualify as arbitration, thus leading to a potentially enforceable award. In cases where it may be possible to qualify the procedure as a form of arbitration, the question arises as to whether certain uses of technology may nonetheless lead to a denial of recognition and enforcement of the resulting award, and why. These issues are discussed in Section 4. Section 5, in turn, looks at future possible applications of blockchain technologies facilitating the recognition and enforcement of court judgments and arbitral awards. Finally, Section 6 concludes.

© PIETRO ORTOLANI, 2023 | DOI:10.1163/9789004514850_023
This is an open access chapter distributed under the terms of the CC BY-NC-ND 4.0 license.

Before delving further into the topic, a terminological clarification is in order. A recurring thread appears throughout the chapter: many of the dispute resolution procedures that are currently being devised in connection with blockchain technologies may well not fit within any of the legal labels that are traditionally used to designate dispute resolution procedures (*i.e.* arbitration, litigation, *etc.*). For this reason, the words "award" and "judgment" would be insufficient to encompass the outcome of some of these procedures. In light of this, the chapter uses the phrase "dispute resolution outcome" as a broader label, encompassing not only outcomes that may qualify as either judgments or (more realistically) arbitral awards, but also other decisions which may not fall within any traditional dispute resolution category.

2 An Overview of the Currently Existing Blockchain Applications for Dispute Resolution

2.1 *The First Use-Case: Routine Escrow Mechanisms on the Bitcoin Blockchain*

In order to grasp the relevance of blockchain technologies for the recognition and enforcement of a dispute resolution outcome, it is useful to look at the first blockchain use-case ever: Bitcoin. Bitcoin is relevant not only because of its importance as a source of inspiration and, to a certain extent, an "archetype" for all other blockchains. In addition, the Bitcoin white paper makes a clear reference to private adjudication, although it never mentions arbitration explicitly. More specifically, Bitcoin was initially conceived as a new "peer-to-peer electronic cash system."[1] In the intentions of the anonymous author(s),[2] Bitcoin was to enable users to make payments without relying on any centralised trusted third party (such as central banks, commercial banks, or payment service providers), and without necessarily disclosing their identity.[3] According to the white paper, Bitcoin would facilitate "commerce on

1 Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (*Bitcoin*) <https://bitcoin.org/bitcoin.pdf> accessed 28 June 2023.

2 The name "Satoshi Nakamoto" is widely considered to be a pseudonym. See, for a journalistic account of the creation of Bitcoin, Nathaniel Popper, *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money* (New York: Harper 2016).

3 It would not be accurate to describe the Bitcoin system as completely anonymous; in fact, users often hold bitcoin without concealing their identity in any way. However, the system does allow users to hold wallets (the Bitcoin equivalent of bank accounts) without revealing their names.

the Internet,"[4] by allowing users to pay for goods and services with a blockchain-based cryptocurrency, instead of fiat currencies issued by central banks, which were perceived as inefficient in many ways.[5] To date, the original vision of author(s) of the white paper has not come into fruition: rather than being a widespread "electronic cash system" or mode of payment, bitcoin is mainly exchanged and held for investment purposes. Nevertheless, it is instructive to look at the original proposal of the Bitcoin white paper, because the author(s) attempt to answer a question which is key to the topic of this chapter: how can an adequate level of user protection be ensured in the absence of any centralised intermediary?

As already mentioned, the Bitcoin white paper is mainly concerned with users entering into commercial transactions on the Internet. Needless to say, such users must be adequately protected: e-commerce is only viable on a large scale if users can rely on effective and inexpensive dispute resolution mechanisms, to enforce their rights. These mechanisms, in turn, foster trust among users operating in electronic marketplaces. By way of example, in a sales contract concluded online, a buyer may fear that the seller will receive the payment of the price, but fail to deliver the goods. At the same time, the seller may be reluctant to deliver the goods if the buyer has not paid the price yet. These fears are magnified in cases where the parties do not personally know each other and are located in different parts of the world. In an "off-chain" transaction (*i.e.* a transaction that is not carried out on a blockchain), several third parties contribute to resolving this problem, meeting the demand for protection (and dispute resolution) that is unavoidably generated by large-scale electronic commerce. In this case, payment service providers protect their users. By way of example, credit card providers can operate a "chargeback," reversing a payment in case of fraud or failure to perform on the part of a trader. Along similar lines, e-commerce platforms such as Amazon and eBay, as well as payment intermediaries such as PayPal, offer dispute resolution services.[6] On top

4 Nakamoto (n 1), 1.

5 *Id.*

6 Ethan Katsh and Orna Rabinovich-Einy, *Digital Justice: Technology and the Internet of Disputes* (Oxford: Oxford University Press 2017); Pablo Cortés, *The Law of Consumer Redress in an Evolving Digital Market: Upgrading from Alternative to Online Dispute Resolution* (Cambridge: Cambridge University Press 2017); Ayelet Sela, "The Effect of Online Technologies on Dispute Resolution System Design: Antecedents, Current Trends and Future Directions" (2017) 21 Lewis & Clark Law Review 633; Louis F. Del Luca, Colin Rule, and Kathryn Rimpfel, "eBay's De Facto Low Value High Volume Resolution Process: Lessons and Best Practices for ODR Systems Designers" (2014) 6 Arbitration Law Review 204; Pablo Cortés, *Online Dispute Resolution for Consumers in the European Union* (Abingdon-on-Thames: Routledge 2011).

of that, the possibility of court litigation and existence of well-functioning alternative dispute resolution (ADR) schemes contribute not only to the resolution of disputes, but also to the prevention thereof, by deterring the parties against non-compliance. In short, off-chain electronic commerce is facilitated by a host of third parties, whose services provide a "safety net" for the contracting parties.

In a blockchain-based decentralised system, by contrast, no such third party exists, and the two parties to a commercial relationship interact with each other directly on a peer-to-peer basis. As a result, no mechanisms such as chargebacks are available,[7] and no in-built safety net exists. Additionally, users engaging in a transaction denominated in Bitcoin may well not be aware of each other's real identity, given the fact that the technology does not require the users to disclose their name or other personal data. As a result, a party may be practically unable not only to seek out-of-court dispute resolution, but also to initiate court proceedings and seek redress from the counterparty, for example for an alleged failure to perform contractual obligations. The Bitcoin white paper addresses these concerns with a short, somewhat cryptic sentence: "routine escrow mechanisms could easily be implemented to protect buyers."[8] This expression alludes to the possibility for users to use the Bitcoin protocol to set up arrangements more complex than a simple transfer of funds from one wallet to another. These arrangements aim to ensure that neither party to a transaction will be able to unilaterally withdraw funds, without the counterparty's consent. While different techniques exist to set up such a mechanism on the Bitcoin blockchain,[9] a widely used one is the so-called multi-signature wallet. Once funds have been stored in a multi-signature wallet, neither party will be able to unilaterally access the cryptocurrency. With a certain degree of approximation, a multi-signature wallet may be described as a lock with two keyholes. Buyer and seller are given one key each; as a result, the seller will be able to verify that the buyer has initiated the payment of the price, but will not be able to withdraw the funds until the goods have been delivered. If no dispute arises, the two parties will then be able to jointly instruct the multi-signature mechanism to release the funds, which will be transferred to the seller's wallet. If, instead, a dispute arises, a third-party adjudicator can be

7 Immutability is one of the oft-quoted distinctive features of blockchain technologies, so that transactions recorded on a blockchain cannot be easily reversed: Primavera de Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Cambridge: Harvard University Press 2017), 33.

8 Nakamoto (n 1), 1.

9 For an overview of possible techniques, see Pietro Ortolani, "Self-Enforcing Online Dispute Resolution: Lessons from Bitcoin" (2016) 36 Oxford Journal of Legal Studies 595.

requested by either party to resolve the dispute. The adjudicator will hear the parties, make a determination, and instruct the mechanism to send the funds stored in escrow either to the seller or to the buyer. The third-party adjudicator, much like the two disputing parties, is provided with a key to the escrow wallet; as a consequence, he/she cannot typically[10] withdraw the funds either, but can unlock the funds by using his/her own key together with the key of the party that prevailed in the private dispute resolution procedure, so that said party will be able to access the funds. Importantly, the possibility of such a multi-signature-enabled private adjudication mechanism is not merely theoretical but is, to the contrary, routinely deployed within different specific communities, which use Bitcoin as a means of payment.[11]

The use of a blockchain-based escrow, while not widespread outside of specific communities, makes for an interesting proof-of-concept: since their inception, blockchain technologies allow for forms of private adjudication which can be described as "self-enforcing." In other words, whenever a private adjudicator resolves a dispute between two parties by determining the destination of funds stored in an escrow wallet, the decision is automatically given effect on the Bitcoin blockchain, despite the fact that it may not be regarded as a legally enforceable dispute resolution outcome. In fact, the issuance of the decision and its enforcement may well factually coincide: the adjudicator may communicate his/her decision by simply directing the disputed sum of money to the wallet of the prevailing party, so that the dispute resolution outcome is immediately implemented on the blockchain. As a consequence, the outcome may not meet the requirements to qualify as an arbitral award, and may in fact be entirely devoid of legal effects. Nevertheless, that outcome may well be executed on the blockchain, by way of technology (rather than through a recognition and enforcement procedure). Importantly, this type of self-enforcement is only possible if the dispute resolution outcome concerns assets that circulate on a blockchain. Hence, in the example above, it will be possible to use the blockchain to ensure the transfer of cryptocurrency to the prevailing party, but not to force the transfer of physical goods which do not circulate on a blockchain. Section 4 will expand on this theme, focusing on the

10 Different escrow techniques allow for different degrees of protection against the risk that the adjudicator will steal the funds stored in the escrow wallet, as observed in *id.*, 610.

11 Bitcoin is used in certain niches of e-commerce, mainly among cryptocurrency enthusiasts (see Pietro Ortolani, "The Three Challenges of Stateless Justice" (2016) 7 Journal of International Dispute Settlement 596), as well as on darknet marketplaces (Sesha Kethineni, Ying Cao, and Cassandra Dodge, "Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes" (2018) 43 American Journal of Criminal Justice 141).

relationship between the qualification of a certain dispute resolution outcome as an arbitral award, and its *de facto* enforceability on the blockchain. Before delving deeper on these issues, however, it is necessary to describe some further use-cases.

2.2 *Beyond Bitcoin: Smart Contracts and Digital Assets*

In the wake of Bitcoin, blockchain technologies have attracted enormous attention, and innumerable other blockchains have been created, with a wide range of purposes and applications. While it is impossible to provide a comprehensive overview of the evolution of blockchain technologies within the limits of this chapter, it is useful to point out two developments, which are relevant to the problem whether a blockchain-based dispute resolution outcome may be recognised and enforced and, if so, under which regime.

The first relevant development is the rise of smart contracts. The definition of smart contracts is controversial, with multiple theories of the legal qualification and relevance of the term being proposed in the literature.[12] For the purposes of this chapter, it suffices to note that, while the Bitcoin protocol is quite rudimentary and only allows the users to transfer coins, or to enter into basic arrangements (such as the aforementioned routine escrow mechanisms), other protocols offer more extensive possibilities to encode an agreement on a blockchain. The most important example in this respect is Ethereum, which offers the users a programming language (Solidity) precisely for the purpose of developing smart contracts. Through these tools, the parties can (to a variable extent) automate certain aspects of a transaction. By way of example, a smart contract may be instructed to perform a payment in the future, only if and when a certain event (*e.g.* contractual performance by the other party) takes place. Furthermore, the smart contract can be instructed to retrieve information that is available outside of the blockchain, and use that information (so-called "oracle") to determine how the contract should be performed. By

12 Kelvin Low and Eliza Mik, "Pause the Blockchain Legal Revolution" (2020) 69 International and Comparative Law Quarterly 135; Mateja Durovic and André Janssen, "Formation of Smart Contracts," in Larry A. DiMatteo, Michel Cannarsa, and Cristina Poncibò (eds), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (Cambridge: Cambridge University Press 2019), 61; Anthony Casey and Anthony Niblett, "Self-Driving Contracts" (2017) 43 Journal of Corporation Law 1; Max Raskin, "The Law and Legality of Smart Contracts" (2017) 1 Georgetown Technology Review 305; Eric Tjong Tjin Tai, "Juridische aspecten van blockchain en smart contracts" (2017) 54 Tijdschrift voor Privaatrecht 563; Kevin Werbach and Nicolas Cornell, "Contracts Ex Machina" (2017) 67 Duke Law Journal 313; Eliza Mik, "Smart contracts: terminology, technical limitations and real world complexity" (2017) 9 Law, Innovation and Technology 269.

way of example, a smart contract may retrieve information about the time of departure and arrival of an airplane, in order to determine whether a transport contract has been performed in accordance with the parties' agreement.

Importantly, a smart contract can be used to automate the enforcement of a dispute resolution procedure, as sub-section 2.3 will describe in further detail. In a nutshell, the potential of self-enforcement that already existed within the Bitcoin blockchain (through escrow mechanisms) is now magnified within other blockchains, whose protocols allow for more complex expressions of private autonomy, *i.e.* smart contracts.

The second relevant development is the proliferation of digital assets. While Bitcoin was initially conceived as an "electronic cash system," other blockchains enable the circulation of other types of digital assets (often referred to as "crypto assets"), which are not meant to operate as a currency. A good example in this respect is the wide range of tokens circulating on the Ethereum blockchain, as well as on other blockchains. This phenomenon gives rise to complex legal issues (especially concerning the legal qualification of tokens, and the consequences thereof),[13] which are not directly relevant for the topic of this chapter. Nevertheless, it is important to note that the rise of crypto assets (be them tokens resembling financial instruments, non-fungible tokens, or other) extends the possibility of ensuring the automatic execution of a dispute resolution outcome on a blockchain. Take the example of two users entering into a contract whereby a token (circulating on the Ethereum blockchain) is to be exchanged against a certain amount of ether (the cryptocurrency of the same blockchain). In this case, both assets involved in the transaction (the token and the cryptocurrency) circulate on the same blockchain. A dispute resolution outcome, hence, may be given effect by way of technology, irrespective of whether it mandates a transfer of cryptocurrency, of the token, or both. In a nutshell, if the range of assets circulating on a blockchain grows in size and variety, this increases the possibility to devise dispute resolution mechanisms where the outcome is given effect through technological means, without the need to rely on recognition and enforcement procedures, and on the intermediation of courts and enforcement authorities (*e.g.* bailiffs) that those procedures traditionally entail.

13 For a comparative analysis of such qualifications see Raffaele Battaglini and Davide Davico, "Is the Crowdfunding Regulation Future-Proof? Forms of Blockchain-based Crowdfunding Falling Outside of the Scope of the Regulation," in Pietro Ortolani and Marije Louisse (eds), *The Crowdfunding Regulation* (Oxford: Oxford University Press 2021) (forthcoming).

2.3 *Smart Dispute Resolution Based on Game Theoretic Incentives*

The growth of blockchain technologies outlined in the previous sub-section has spurred the proliferation of a number of online dispute resolution mechanisms which aim to ensure the implementation of an outcome, without the need to rely on traditional recognition and enforcement procedures. These mechanisms often operate as "oracles:" the outcome of the dispute resolution procedure will be fed into a smart contract, which will in turn give effect to the outcome on the blockchain. For this reason, these mechanisms are sometimes labelled as "smart dispute resolution."[14] The adjective "smart," however, should not be read as suggesting that these mechanisms rely on automated decision-making or artificial intelligence. In other words, the dispute is typically not resolved by a smart machine operating as a sort of "robo-arbitrator;" to the contrary, most of these systems rely on human decision-making, and are based on a game theoretical framework, as this sub-section will illustrate. The word "smart," hence, simply suggests a certain degree of automation in the implementation of the dispute resolution outcome, rather than in its creation. The market for these new forms of dispute resolution is quite fluid, with new products entering the scene at any given moment, and other ones being discontinued. For this reason, rather than providing an in-depth description of each single smart dispute resolution procedure currently available, this sub-section will offer an overview of the core features that many of these procedures share.

Typically, smart dispute resolution mechanisms are aimed at small-value, high-volume disputes, for which traditional dispute resolution avenues would not be a viable option.[15] Smart dispute resolution is normally advertised not as a binding form of arbitration, but as a sub-category of online dispute resolution (ODR), the practical effectiveness of which relies on the underlying technology, rather than on the legal enforceability of the outcomes it leads to. In other words, within the context of smart dispute resolution, the allocation of the disputed assets to the prevailing party is supposed to be guaranteed by technology (typically, sending cryptocurrency or tokens to the wallet of the party that prevailed in the procedure). From this point of view, smart dispute resolution is comparable to the aforementioned dispute resolution schemes offered by e-commerce platforms,[16] as well as the private adjudication of domain-name

14 Alessandro Palombo, Raffaele Battaglini, and Luigi Cantisani, "A Blockchain-Based Smart Dispute Resolution Method," in Larry A. DiMatteo et al. (eds), *The Cambridge Handbook of Lawyering in the Digital Age* (Cambridge: Cambridge University Press 2021), 122.

15 Mateja Durovic and Franciszek Lech, "Legal Tech in ADR," in Larry A. DiMatteo et al. (eds), *The Cambridge Handbook of Lawyering in the Digital Age* (Cambridge: Cambridge University Press 2021), 99.

16 See Ortolani (n 9) above and accompanying text.

disputes.[17] Although none of these mechanisms are purported to produce *res judicata* effects, or to lead to the issuance of an enforceable title (such as an arbitral award), the dispute resolution outcome is implemented through technological means. As a result, these procedures do not prevent the unsuccessful party from re-litigating the case: were, for example, court proceedings to be initiated, the seized court would be able to disregard the outcome of the ODR procedure altogether, and hear the case *de novo*. In practice, however, this is a relatively rare occurrence, given the typically small value of the disputes. Another recent example of this trend of "enforcement through technology" is visible in the realm of social media, where disputes about the limits of freedom of expression on social media platforms are adjudicated by the platforms themselves, or occasionally by quasi-judicial bodies set up by the platforms.[18] While the users remain free to re-litigate these cases, the decision made by the platform is likely to undergo no judicial scrutiny in the vast majority of cases.

Many smart dispute resolution schemes are based on a game theoretical framework. The reason for such a framework is that, as already mentioned, these procedures are aimed at resolving a high volume of low-value cases. To make this goal attainable, it is necessary to limit the costs of adjudication, since it would not be viable for the parties to bear the costs associated with a traditional arbitration. To this end, smart dispute resolution mechanisms typically allow the users themselves to act as voters, expressing their views on disputes that have been submitted for resolution. More specifically, a "crowd" of users is allowed, under certain conditions, to cast votes on what they believe the "correct" outcome of the dispute should be. This, of course, raises a wide range of delicate questions. Just to mention some of the most obvious issues, how can the "correct" outcome be identified? How can the independence and impartiality of adjudication be preserved, if a wide range of users is able to cast votes? And how can the quality of decision-making be ensured? Smart dispute resolution aims at resolving these problems by placing the users within

17 See for instance Internet Corporation for Assigned Names and Numbers (ICANN), "Uniform Domain Name Dispute Resolution Policy" (*ICANN*, 24 October 1999) <https://www.icann.org/resources/pages/policy-2012-02-25-en> (UDRP).

18 Lorenzo Gradoni, "Constitutional Review via Facebook's Oversight Board: How platform governance had its Marbury v Madison" (*Verfassungsblog*, 10 February 2021) <https://verfassungsblog.de/fob-marbury-v-madison/>; Kate Klonick, "The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression" (2020) 129 Yale Law Journal 2418; Evelyn Douek, "Facebook's Oversight Board: Move Fast with Stable Infrastructure and Humility" (2019) 21 North Carolina Journal of Law and Technology 1; Kate Klonick, "The New Governors: The People, Rules, and Processes Governing Online Speech" (2018) 131 Harvard Law Review 1598.

a system of economic incentives, designed to disincentivise biased or corrupt behaviour. While each of these systems has its specific features, for the purposes of this chapter, some common traits can be identified.

The dispute resolution procedure typically lasts for a limited number of days. At the outset, the disputing parties present their arguments in writing, together with the evidence they rely upon.[19] Subsequently, the jurors are allowed to read the arguments, evaluate the evidence, and cast votes, indicating which party should prevail. Votes are cast by committing a specific type of token, which must be purchased in advance. Once a vote is cast, the tokens are "frozen," and the user will not be able to claim them back until the procedure is concluded. In some dispute resolution schemes, users are only allowed to cast votes if they hold a certain amount of tokens, and/or if they demonstrate a certain level of expertise.[20] Furthermore, in some mechanisms, the voters will be required to provide a brief reasoning for their vote.[21] In other schemes, instead, no such barriers or requirements exist.[22] Importantly, a user holding more tokens will be able to cast a higher number of votes.[23] After the time-frame for the procedure has elapsed, the disputing party obtaining the majority of the votes will prevail, and obtain the disputed assets (*e.g.* a certain amount of cryptocurrency, which will automatically be transferred to that party's wallet). The voters who find themselves in the majority will obtain their tokens back, together with an additional amount of tokens coming from the minority voters. By contrast, those who voted for the unsuccessful party will lose their tokens (which will be redistributed among the majority voters). In the intention of the designers of these systems, this framework of economic incentives will "crowd out" biased or bad-faith behaviour. In other words, according to the white papers promoting these systems,[24] it may well be possible that some users will vote in a biased way, favouring a disputing party that should not prevail. The other users, however, will have an economic incentive to act in good faith, pool their tokens, and vote for the other party, so as to form a majority and gain the minority's tokens. This, in turn, is supposed to disincentivise the users from voting for an outcome that they deem to be incorrect, since this may result in the total loss of the tokens used to cast such votes.

19 Orna Rabinovich-Einy and Ethan Katsh, "Blockchain and the Inevitability of Disputes: The Role for Online Dispute Resolution" (2019) 2 Journal of Dispute Resolution 47, 59–71.

20 See *e.g.*, *Kleros*: *id.*, 60.

21 See *e.g.*, *Juris*: *id.*, 62.

22 See *e.g.*, *Jur Open Layer*: https://jur.io/products/open-layer/.

23 Durovic and Lech (n 15); Rabinovich-Einy and Katsh (n 19).

24 Durovic and Lech (n 15), 113–120.

The rapidly evolving universe of smart dispute resolution still leaves many questions unanswered. Many smart dispute resolution systems are based on the premise that the users will be able not only to understand a dispute (despite the potential lack of any legal background), but also to univocally identify which of the disputing parties should succeed, so that a majority of good-faith users will prevail over the minority and, as a consequence, reap a profit. To date, such premise remains questionable: many disputes, even when the value is relatively low, may be open to different possible lines of reasoning, which may in turn lead to diverging outcomes. Such uncertainty is compounded by the assumption that the dispute should not be resolved according to any specific set of legal rules (with which the users would likely be unfamiliar), but pursuant to general notions of fairness and equity, which are inherently vague as well as dependent on many variables (such as cultural specificities). In addition, the disputing parties are required to present their arguments in writing, and prove them with documentary evidence within a very short time-frame. This, of course, may favour one of the disputants, who may be able to rely on such type of evidence, to the detriment of the opponent, who may well need oral evidence to prove his/her arguments. Furthermore, more general and policy-driven objections could be raised. In particular, it may be argued that these systems contribute to a dangerous "gamification" of dispute resolution, transforming private adjudication into a game to be played for economic purposes, rather than a function to be performed in the pursuit of justice.[25] Next to these general concerns, system-specific objections could be raised for each of the existing smart dispute resolution mechanisms: depending on the specific features of each game theoretical framework, the system may well be unable to work in practice, and to deliver acceptable outcomes, simply because the economic incentives of the system are not sufficient to disincentivise bad-faith behaviour. For the purposes of this chapter, however, all of these lines of inquiries can simply be taken as a background, against which the main question will be scrutinised: given that these systems exist, to what extent and how do they interact with recognition and enforcement procedures? Sections 3 and 4 will answer this question. However, before delving into these matters, it is necessary to briefly describe one last development at the intersection between blockchain and dispute resolution: the rise of blockchain-based arbitration.

25 Amy Schmitz and Colin Rule, "Online Dispute Resolution for Smart Contracts" (2019) Journal of Dispute Resolution 103, 118.

2.4 *Blockchain-based Arbitration*

The smart dispute resolution procedures summarised in the previous sub-section cannot, by their very nature, be used to resolve all types of disputes. Even if one were to accept the theoretical premises of these systems, and disregard the doubts they raise, surely these mechanisms cater to disputing parties seeking a fast and inexpensive resolution of a dispute that will normally be low in value, and not to those in need of experienced and reliable adjudicators. The typical party to a mid-value commercial transaction will not accept to refer disputes to the vote of a crowd of users with no legal background, acting on the basis of their own economic interests. In other words, the rise of smart dispute resolution may enable the adjudication of disputes that are too small to end up in "traditional" arbitration or litigation, but it does not constitute a convincing model for larger and more complex cases. It is precisely this observation that has spurred yet another development at the crossroads between blockchain and dispute resolution, namely blockchain-based arbitration.

Some of the projects that are currently being developed aim to create procedures that are based on blockchain technology, but at the same time qualify as arbitration, combining the advantages of both. In other words, according to the developers, these procedures would rely on the framework of distributed ledger technologies, but would also constitute arbitration, hence leading to *res judicata* effects and to legally enforceable awards.[26] There is an obvious appeal in the idea of combining the "best of both worlds:" on the one hand, blockchain may make arbitration more efficient, and ensure compliance with the award by technological means. On the other hand, the qualification of the procedure as an arbitration (and of the outcome as an arbitral award) guarantees that the dispute resolution procedure will be able to produce not only "on-chain" effects, but also "off-chain" ones. Therefore, by way of example, the unsuccessful party would not be able to simply disregard the dispute resolution outcome, and require that the case be heard *de novo* by either a court or a new arbitral tribunal. Furthermore, the award would be enforceable, *inter alia* under the 1958 New York Convention, so that traditional enforcement procedures may be available, at the behest of the award creditor, whenever "on-chain" compliance by way of technology will not be possible.

26 See *e.g.*, *Mattereum*, a blockchain-based platform aimed at facilitating commerce in physical assets and the resolution of related disputes through legally binding arbitration (Matterum, "Powering a Circular Economy for a world drowning in goods" (*Mattereum*) <https://mattereum.com> accessed 28 June 2023), or *Jur*, applying blockchain technologies to different aspects of the arbitral process, to enhance speed and efficiency (Jur, "The New Jurisdiction For The Digital Economy" (*Jur*) <https://hi.jur.io/> accessed 28 June 2023).

Despite the attractiveness of the idea of blockchain-based arbitration, its practical implementation may prove arduous. As explained in the previous sub-sections, one of the advantages of blockchain-based dispute resolution is that the implementation of the outcome is not dependent on the voluntary compliance of the unsuccessful party, or on cumbersome recognition and enforcement procedures. To the contrary, the technology itself ensures that the disputed assets be delivered to the prevailing party. However, as already mentioned, this entails some crucial requirements. First of all, the disputed assets must circulate on a blockchain, with which the dispute resolution mechanism must be able to communicate (typically through a smart contract retrieving information from an oracle); on-chain implementation, conversely, is not possible, if the dispute resolution outcome (*e.g.* the arbitral award) grants any type of off-chain relief, such as the delivery of assets that do not circulate on a blockchain. In addition, on-chain implementation of a dispute resolution outcome can only happen if and inasmuch as the parties have made it possible. For instance, a smart contract may perform a transfer of cryptocurrency from an escrow wallet to the wallet of the prevailing party only if the cryptocurrency has been previously stored in the escrow wallet. Along similar lines, if a dispute arises over the ownership of a token, it will be possible to ensure that the token will automatically be transferred to the prevailing party only on the condition that a smart contract has been previously authorised to make such transfer.

In practice, the aforementioned requirements may prove to be a significant bottleneck for disputes that are not particularly low in value. A comparison with traditional arbitration may be useful to clarify this point. Suppose that two parties enter into a commercial contract and agree to arbitrate any dispute arising out of or in connection with that contract. In order to ensure that any arbitral award will be promptly complied with, the parties set up a security bank account, where both of them deposit a sufficient amount of money to pay any award made against either party by an arbitral tribunal. The parties will not be able to withdraw money from the bank account without the consent of an escrow agent, whom the parties jointly appoint for the management of the security account. This type of arrangement is not unprecedented; to the contrary, it is precisely such a security account that guarantees the payment of awards issued by the Iran-US Claims Tribunal.[27] Nevertheless, this model is obviously not viable for most parties routinely entering into commercial contracts, given the parties' need to maintain liquidity for a wide range of

27 David D Caron, "The Nature of the Iran-United States Claims Tribunal and the Evolving Structure of International Dispute Resolution" (1990) 84 The American Journal of International Law 104, 129.

unrelated purposes in the course of business. In other words, if agreeing to arbitrate would entail the need to freeze significant amounts of money until the underlying contract has been performed, arbitration would clearly become unviable in practice. When transposing this example to the blockchain world, the same economic considerations apply: two contracting parties would be unlikely to freeze a non-negligible amount of cryptocurrency in an escrow wallet for a long period of time, for the sole purpose of ensuring the enforcement of dispute resolution outcomes. The volatility of many cryptocurrencies is an additional deterrent in this respect.

Despite these significant limitations, the prospect of blockchain-based, self-enforcing arbitration is not entirely utopic, at least for certain categories of crypto assets. By way of example, blockchain developers are currently exploring the possibility of creating non-fungible tokens, which are supposed to represent legal title to physical assets existing off-chain.[28] Were a dispute to arise concerning the ownership of such assets, it may be possible to "freeze" the token until the conclusion of a blockchain-based arbitral procedure, without at the same time curtailing the possibility of using the physical assets. For instance, the token representing the right of property over a piece of machinery may be put in escrow on the blockchain, but the party having possession of that piece of machinery would still be able to use it while the blockchain-based arbitration is pending. Once again, it should be stressed that the world of blockchain is rapidly evolving, and further examples may arise in the near future. In light of this, the possibility of blockchain-based arbitration should not be dismissed as unrealistic just yet.

3 Identifying the Regime Governing Recognition and Enforcement

3.1 *Relevance of the Problem of Legal Qualification of the Procedure*

The analysis carried out so far has shown how blockchain technologies have given rise to a range of dispute resolution mechanisms, which differ from each other in crucial ways. For this reason, it is impossible to reach a general conclusion as to whether the outcome of such a mechanism may be recognised and enforced pursuant to the regime applicable for example to arbitral awards. To the contrary, the answer will necessarily be case-specific, and contingent on the features of each particular dispute resolution mechanism. In other words, it is first of all necessary to legally qualify each dispute resolution mechanism,

28 See for instance *Mattereum*, (n 26).

in order to then determine which recognition and enforcement regime (if any at all) will be applicable.

In general terms, it is often easier to identify a court judgment than an arbitral award:[29] while the former is issued by a national court, *i.e.* a public institution forming part of the constitutional architecture of a given state, arbitration remains to a certain extent a fluid label, encompassing a range of private adjudication phenomena sharing certain characteristics. To date, no national legal system has integrated their courts with blockchain technologies to such an extent to support the hypothesis that a dispute resolution outcome on a blockchain may qualify as a judgment. This state of affairs may change in the near future, as Section 5 will illustrate. For the time being, however, the main practically relevant question is whether a blockchain dispute resolution outcome may be recognised and enforced as an arbitral award. This, in turn, raises the question of what is an arbitral award for the purposes of the 1958 New York Convention, as well as under the other regimes that may enable the circulation of awards.

3.2 *Circumstances That Are Not Relevant for the Qualification of the Procedure*

In this respect, it is useful to start from a survey of circumstances that are *not* relevant for the qualification of a dispute resolution as an arbitral award. First of all, the circumstance that a certain document qualifies itself as an arbitral award is not determinative of its nature. There are, in fact, numerous instances of dispute resolution outcomes that are formally labeled as "awards," but may well not qualify as such. A good example are decisions issued by emergency arbitrators (as well as, more generally, decisions issued by arbitral tribunals which are designated as "awards" by the arbitrators, but only grant provisional or interim forms of relief). In the literature, diverging views have been expressed as to whether emergency arbitrators decisions qualify as arbitral awards.[30] This

29 To be sure, there are cases which blur the boundaries between the two: judgments issued by the Dubai International Financial Centre (DIFC) Courts, for instance, can be entered into arbitral awards for the purposes of their international circulation under the New York Convention: Dalma R. Demeter and Kayleigh M. Smith, "The Implications of International Commercial Courts on Arbitration" (2016) 33 Journal of International Arbitration 441.

30 Jakob Horn, "The Emergency Arbitrator Under the New York Convention" (2021) 31 The American Review of International Arbitration; Rajesh Kapoor, "The Concept of Arbitral Award Under the New York Convention: A Comparative Study of English, French and Indian Approaches," in Mathew John et al. (eds), *The Indian Yearbook of Comparative Law* (Springer Singapore 2019), 39; Rafael Dean Brown, "Challenging the Enforcement of Emergency Arbitrator Decisions" (2021) 8 Kuwait International Law School Journal 39;

disagreement largely depends on the different possible interpretations of what constitutes an arbitral tribunal, and whether the decision is binding upon the disputants and final.[31] For this reason, national courts requested to enforce emergency arbitral decisions have taken opposite views, with some of them showing willingness to treat these decisions as awards,[32] and other ones rejecting such a qualification.[33] A similar debate exists with respect to awards by consent issued after a mediation procedure, with the purpose of ensuring the enforceability of a settlement agreement reached by the parties.[34] Applying this line of reasoning to a blockchain-based dispute resolution outcome, it is irrelevant whether a certain procedure has been advertised as a form of legally binding arbitration or not. Hence, representations made in "white papers," such as the ones summarised above in section 2, are not conclusive in this respect.

Sai Ramani Garimella and Poomintr Sooksripaisarnkit, "Emergency Arbitrator Awards: Addressing Enforceability Concerns Through National Law and the New York Convention," in Katia Fach Gomez and Ana M. Lopez-Rodriguez (eds), *60 Years of the New York Convention: Key Issues and Future Challenges* (Alphen aan den Rijn: Kluwer Law International 2019), 67; Erika Donin, Isabelle Bueno, and Vitoria Campos, "The Enforceability of Emergency Arbitrator's Decisions under the New York Convention" (2018) Young Arbitration Review; Jaroslav Kudrna and Ank Santens, "The State of Play of Enforcement of Emergency Arbitrator Decisions" (2017) 34 Journal of International Arbitration 1; Diana Paraguacuto-Maheo and Christine Lecuyer-Thieffry, "Emergency Arbitrator: A New Player in the Field - The French Perspective" (2017) 40 Fordham International Law Journal 749; Fabio G. Santacroce, "The emergency arbitrator: a full-fledged arbitrator rendering an enforceable decision?" (2015) 31 Arbitration International 283; Baruch Baigel, "The Emergency Arbitrator Procedure under the 2012 ICC Rules: A Juridical Analysis" (2014) 31 Journal of International Arbitration 1; Amir Ghaffari and Emmylou Walters, "The Emergency Arbitrator: The Dawn of a New Age?" (2014) 30 Arbitration International 153; Patricia Shaughnessy, "Pre-arbitral Urgent Relief: The New SCC Emergency Arbitrator Rules" (2010) 27 Journal of International Arbitration 337.

31 Santacroce (n 30), 303.

32 BayObLG München, 18 August 2020 – 1 Sch 93/20; *Sharp Corp. v. Hisense USA Corp.*, 292 F. Supp. 3d 157 (D.D.C. 2017); *Yahoo v. Microsoft*, 983 F. Supp. 2d 310 (S.D.N.Y. 2013); *Draeger Safety Diagnostics v. New Horizon Interlock*, (E.D. Mich. 2011), WL 653651; *Blue Cross Blue Shield of Michigan v. Medimpact Healthcare Systems*, (E.D. Mich. 2010), WL 2595340.

33 *Raffles Design International India Pvt. Ltd.& Anr. v. Educomp Professional Education Ltd.& Ors.* (MANU/DE/2754/2016); *Société Nationale des pétroles du Congo et République du Congo v. Société Total Fina Elf E&P Congo*, Paris Court of Appeal, 29 April 2003, *Revue de l'Arbitrage* (2003): 1296.

34 Giacomo Marchisio, "A comparative analysis of consent awards: accepting their reality" (2016) 32 Arbitration International 331; Stacie Strong, "Beyond International Commercial Arbitration? The Promise of International Commercial Mediation" (2014) 45 Washington University Journal of Law and Policy 11; Christopher Newmark and Richard Hill, "Can a Mediated Settlement Become an Enforceable Arbitration Award?" (2000) 16 Arbitration International 81.

Furthermore, practice also shows instances of procedures that do resemble arbitration in some way, but lead to decisions which uncontroversially do not qualify as arbitration. An interesting example is the aforementioned case of domain-name dispute resolution: although this is a private adjudicative procedure, often administered by an arbitral institution, the outcome does not qualify as an arbitral award, and is not enforceable as such.[35] In this respect, it is irrelevant whether the parties have referred to this procedure as a form of arbitration. Private autonomy, in other words, cannot trigger the applicability of a certain recognition and enforcement regime (*e.g.* the 1958 New York Convention) by simply appending a label "arbitration" to a procedure that does not qualify as such. Applying these findings to blockchain-based dispute resolution, the circumstance that the parties have defined as "arbitration" a certain procedure (*e.g.* a private adjudication scheme supported by a blockchain-based escrow mechanism, such as the one described in sub-section 2.1. above) does not ensure that the procedure will indeed be regarded as arbitration by national courts.

3.3 *Circumstances That Contribute to the Qualification of the Procedure*

Having clarified which factors are irrelevant to the qualification of a certain outcome as an arbitral award, it is possible to provide an overview of factors that can instead play a role in this respect. Importantly, the 1958 New York Convention does not provide a definition of "arbitration," and neither do many modern arbitration statutes.[36] Nevertheless, the latter do contain some important indicators. To be sure, these indicators do not "set the bar" at a particularly high level, especially when compared with the requirements for recognition and enforcement; in other words, it is possible for a procedure to meet the minimum requirements to qualify as arbitration, while at the same time leading to an award that may be declined recognition and enforcement, *inter alia* under Article V of the New York Convention. However, some blockchain-based dispute resolution procedures already fail to satisfy these basic requirements, thus precluding the possibility of recognition and enforcement

35 For an analysis of the nature of UDRP decisions see Pietro Ortolani, "Digital Dispute Resolution: Blurring the Boundaries of ADR," in Larry A. DiMatteo et al. (eds), *The Cambridge Handbook of Lawyering in the Digital Age* (Cambridge: Cambridge Unviersity Press 2021), 140, 147.

36 Santacroce (n 30), 302–306. In the absence of any such binding definition, different theoretical frameworks for the identification of arbitration have been put forth in the literature: Charles Jarrosson, *La notion d'arbitrage* (Paris: LGDJ 1987); Bruno Oppetit, *Théorie de l'arbitrage* (Paris: PUF 1998); Jan Paulsson, *The Idea of Arbitration* (Oxford: Oxford University Press 2013).

altogether. In other words, some blockchain-based dispute resolution procedures are best understood as smart dispute resolution schemes which, as illustrated above in sub-section 2.3, do not produce legally binding effects, nor lead to the issuance of enforceable outcomes. By contrast, other schemes may qualify as blockchain-based, legally binding arbitration, thus enabling the award creditor to seek recognition and enforcement. The question, then, is which features of these schemes should be considered in order to determine whether a specific type of blockchain-based procedure qualifies as arbitration. To answer this question from a comparative point of view, references will be made to the UNCITRAL Model Law on International Commercial Arbitration. Needless to say, the inferences drawn from this analysis may vary, were a national arbitration statute to diverge significantly from the Model Law.

Article 2 of the Model Law defines an "arbitral tribunal" as "a sole arbitrator or a panel of arbitrators." Article 10, in turn, specifies that the parties are free to determine the number of arbitrators but, failing such determination, the number of arbitrators shall be three. When read together, these two provisions entail the presence of a pre-determined number of individuals sitting as arbitrators, entrusted with the task of finally resolving the dispute. As illustrated above in sub-section 2.3, many smart dispute resolution mechanisms fail to meet such a requirement, since they enable a crowd of token-holders to cast votes on how the dispute should be resolved. Such an arrangement makes it impossible for the parties not only to determine the number of adjudicators, but also to simply predict how many individuals will cast a vote. This feature, in and of itself, is sufficient to cast serious doubts on the possibility to qualify these mechanisms as arbitration. By contrast, any form of blockchain-based scheme which would refer the dispute to a given number of adjudicators (most frequently, one or three) would seem to comply with the requirements implicitly set forth by Articles 2 and 10 of the Model Law.

Article 12 of the Model Law requires arbitrators to be impartial and independent, allowing challenges where "justifiable doubts" exist. Furthermore, the right to an independent and impartial adjudicator enshrined in Article 6 of the European Convention on Human Rights applies to arbitral proceedings, as long as the parties have not freely waived it in an unequivocal manner.[37] One of the most obvious consequences of the requirement of independence and impartiality is that arbitrators should not have a financial interest in the outcome of the case, as specified *inter alia* by the IBA Guidelines on Conflicts

37 European Court of Human Rights, *Beg S.p.A. v. Italy*, Application no. 5312/11, para. 136; *Mutu and Pechstein v. Switzerland*, Applications nos. 40575/10 and 67474/10, para. 103.

of Interest in International Arbitration.[38] Once again, many smart dispute resolution schemes fail to meet this requirement by their very design. In particular, the game theoretical framework on which many of these schemes are based consists precisely in a set of economic incentives for the token-holders, who will be able to reap a profit only if they select the "correct" solution of the dispute, as illustrated above in sub-section 2.3. The circumstance that the token-holders may gain or lose tokens, depending on how the dispute is resolved, seems impossible to reconcile with the requirements of independence and impartiality set forth not only in arbitration statutes, but also in human rights law.[39] In other words, arbitration is structurally designed so as to ensure the independence and impartiality of arbitrators; these systems, by contrast, are designed so as to present token-holders with favourable or unfavourable economic consequences, depending on how the case will be decided. Hence, smart dispute resolution schemes that aim to "nudge" a crowd of adjudicators through outcome-dependent economic incentives should not be regarded as a form of arbitration. By contrast, a blockchain-based dispute resolution system may qualify as arbitration if the adjudicators are required to resolve the dispute independently and impartially, and their ability to earn a profit is not contingent on which of the disputants will prevail.

A further layer of doubt is raised with respect to the substantive rules or standards pursuant to which the dispute is to be resolved. As already illustrated, several smart dispute resolution mechanisms incentivise their token-holders to cast a vote in accordance with what they perceive to be the "correct" solution, without making reference to any substantive body of law. Such a design feature seems to suggest that the voters should resolve the dispute *ex aequo et bono*. However, pursuant to Article 28(3) of the Model Law, *ex aequo et bono* adjudication is not the rule in arbitration, but rather the exception, only possible if the parties have expressly authorised the tribunal in this sense. Hence, the mere circumstance that the parties have deployed a smart contract is probably insufficient to grant the adjudicators the power to decide the case *ex aequo et bono*. The logical consequence of this line of reasoning is, once again, that these systems of smart dispute resolution should not be qualified as arbitration, at least under the UNCITRAL Model Law. By contrast, if

38 International Bar Association, "IBA Guidelines on Conflicts of Interest in International Arbitration" (*IBA*, 23 October 2014), item 1.3 (Non-Waivable Red List) <https://www.ibanet.org/MediaHandler?id=e2fe5e72-eb14-4bba-b10d-d33dafee8918>.

39 See recently on this point, European Court of Human Rights, (n 37), para. 143, requiring arbitral tribunals to act independently and impartially whenever the parties have not expressly and unequivocally waived these guarantees.

the blockchain-based dispute resolution mechanism is based on an agreement whereby the parties expressly entrust the adjudicators with the task to finally decide the case *ex aequo et bono*, it may in principle be possible to qualify such a procedure as a form of arbitration.

Article 29 of the UNCITRAL Model Law requires that, in arbitrations with more than one arbitrator, any final decision on the merits be made by a majority of the members of the tribunal. This provision requires that all arbitrators have equal voting powers. However, some smart dispute resolution mechanism confer upon the tokenholders a right to cast votes which is proportional to the amount of tokens they hold, so that a user committing more tokens will be able to influence the outcome more than a different user committing less tokens.[40] This is another feature that precludes the qualification of some blockchain-based dispute resolution procedures as arbitration. If, by contrast, the adjudicators all have equal voting powers, such a qualification is in principle possible.

Finally, Article 31 of the UNCITRAL Model Law requires the award to be made in writing and signed by the arbitrators. These requirements are typically not met by smart dispute resolution procedures where the users are allowed to cast a vote (and, depending on the procedure, to provide a reasoning), but not to sign the final outcome. Unlike arbitration, these procedures are clearly not designed to lead to the issuance of a legally enforceable title. By contrast, other blockchain-based dispute resolution procedures may require the adjudicators to issue a written, reasoned decision, and sign it. In this latter situation, the qualification of the outcome as an arbitral award would be possible.

In sum, the analysis carried out so far indicates that the recognition and enforcement of blockchain-based outcomes as arbitral awards is often impossible, for the simple fact that these procedures (such as the ones described above in sub-section 2.3) do not meet the minimum requirements to qualify as arbitration (nor are they *a fortiori* entitled to circulate as court judgments). By contrast, in other dispute resolution mechanisms (such as the ones described above in sub-section 2.4), a pre-determined number of adjudicators is entrusted with the task of finally resolving the dispute in an impartial and independent manner, making determinations by majority, according to the applicable law or other applicable substantive standard, and rendering binding, written, signed and reasoned decisions. A procedure meeting these requirements would, in principle, qualify as arbitration, thus enabling the circulation of the outcome as an arbitral award, *inter alia* under the 1958 New York Convention. Hence, it

40 Durovic and Lech (n 15), 113–120.

is only with reference to this latter group of procedures that it makes sense to investigate whether recognition and enforcement may be declined and, if yes, on the basis of which grounds for refusal.

4 Grounds for Refusal of Recognition and Enforcement

Even if a blockchain-based dispute resolution procedure meets the minimum requirements to qualify as arbitration, certain features of the procedure may generate doubts as to whether the recognition and enforcement of the resulting award may be declined. This section will provide an overview of the doubts that may arise, with specific reference to the New York Convention. To be sure, this overview is not exclusive, but it simply complements the analysis that should ordinarily be carried out to determine whether any arbitral award may be denied recognition and enforcement. In other words, there is a spectrum of circumstances that may lead to a denial of recognition and enforcement, irrespective of whether the arbitration was based on blockchain technologies or not. This section, however, focuses on technology-specific grounds for refusal that may be triggered by particular circumstances, connected to the use of blockchain technologies in the arbitration.

4.1 *Existence of a Valid Agreement to Arbitrate*

Under Article V(1)(a) of the New York Convention, recognition and enforcement may be denied if no valid agreement to arbitrate exists between the parties. By agreeing to arbitrate, the parties waive their fundamental right to access state courts, and submit themselves to a private adjudication mechanism that will result in the issuance of a binding, enforceable award with *res judicata* effects. For these reasons, consent is widely regarded as a prerequisite for arbitration, and the Convention allows a denial of recognition and enforcement if no such consent has been given. This ground for refusal may become relevant whenever the parties have engaged in a blockchain-based dispute resolution procedure, the nature of which is not immediately evident. Let us suppose, for instance, that two contracting parties set up a Bitcoin escrow wallet, as described above in sub-section 2.1, entrusting a third-party adjudicator to determine where the cryptocurrency stored in said wallet should be transferred, were a dispute to arise. Once a dispute materialises, the third-party adjudicator makes a determination that the cryptocurrency should be paid to one of the two disputing parties. After such determination, the unsuccessful party commences court litigation against its counterparty, arguing that the determination of the adjudicator was wrong, and claiming repayment. The successful party appears in

the court proceedings, and argues that the case is *res judicata*, since the adjudicator's determination is in fact an arbitral award, which must be recognised by the seized court. Given these facts, the unsuccessful party may argue that the procedure carried out by the third-party adjudicator was not, in fact, a form of arbitration, for example on grounds outlined above in section 3. Additionally, however, that party may also argue that he/she never consented to submit the case to arbitration and waive access to state courts. More specifically, it could be argued that the parties' decision to set up a Bitcoin escrow wallet does evince their consent to have a third-party adjudicator carry out payments out of that wallet; however, it does not demonstrate that the parties agreed that the adjudicator's decision would be final and binding on them. In the absence of a clear agreement to arbitrate, the adjudicator's decision may be seen as an initial allocation of resources, which the parties remain free to undo or modify, *inter alia* by seeking relief in a competent court. In sum, setting up an escrow mechanism (such as the one described in sub-section 2.1 above) may be sufficient to enable an adjudicator to issue a decision that will automatically be given effect on the blockchain, but it may well be insufficient to demonstrate that the parties intended for that decision to be final and binding, and to circulate as an arbitral award.

4.2 *Notice of Appointment of the Tribunal and of the Arbitral Proceedings*

A further ground for refusal concerns the fact that a party was not given proper notice of the appointment of the arbitrator and of the arbitral proceedings. This ground is potentially relevant for any dispute resolution procedure where a "crowd" of users is allowed to cast votes on the outcome of the dispute. Even if such procedures were to be qualified as a form of arbitration (despite the doubts described in section 4 above), the party resisting enforcement may argue that no proper notice was given of the appointment of the arbitrators, since anybody would be able to cast a vote, as long as they hold tokens in their wallet. Along similar lines, that party may also argue that such a mode of appointment of arbitrators leads to the composition of a tribunal with a variable and unpredictable number of members, so that no meaningful consent to such composition may be given. This, in turn, may be invoked as a ground for refusal, under Article V(1)(d) of the New York Convention.

4.3 *Due Process and the Parties' Fundamental Procedural Rights*

Arbitral awards may be denied recognition and enforcement if the parties' fundamental procedural rights were violated, and if the disputants were not afforded a reasonable opportunity to present their case. Under the New York

Convention, due process violations may be lamented by the party resisting recognition and enforcement under the public policy clause of Article V(2)(b), as well as under Article V(1)(b) (referring to a party "otherwise unable to present his case"). Whether this ground for refusal can be successfully invoked by the award creditor depends largely on how each particular arbitral procedure was carried out; as such, it is impossible to determine in abstract terms whether a blockchain-based arbitral procedure affords sufficient due process guarantees. Nevertheless, it is possible to refer to some recurring characteristics of the procedures that have been described above in section 2. More specifically, some blockchain-based dispute resolution procedures only afford the parties the opportunity to put forth written defenses, and to submit documentary evidence. On the one hand, the fact that an arbitration has been conducted on a documents-only basis does not, *per se*, jeopardise the validity of the award, or the possibility of recognition and enforcement. On the other hand, however, it is normally expected that the parties consent to such a form of arbitration, waiving their right to an oral hearing (for the purposes of both the presentation of oral arguments and for the taking of oral evidence).[41] It will then be important to assess whether the parties could reasonably expect the procedure to be conducted on a documents-only basis when they agreed to arbitrate. Thus, if the arbitration is conducted on the basis of a set of rules which provide for documents-only arbitration, which the parties consented to, the failure to conduct an oral hearing will likely not be sufficient to decline recognition and enforcement of the resulting award. If, by contrast, no such rules are available, and the disputants have not otherwise agreed to arbitrate on a documents-only basis, the failure to conduct an oral hearing may possibly be invoked to justify a denial of recognition and enforcement.

A partially comparable analysis applies to those blockchain-based arbitration procedures that do allow for an oral hearing, but provide that the hearing will be conducted via videoconference, rather than in person.[42] Once again, the parties' consent to a set of rules which provides for a so-called "virtual" hearing should be sufficient to rule out the possibility of a denial of recognition and enforcement, and the same holds true for situations where the parties consented to a virtual hearing at the beginning of the procedure (*e.g.* by subscribing to the terms of reference, or to procedural order no. 1). By contrast, delicate problems may arise in situations where the tribunal orders a virtual hearing in the absence of an agreement of all disputing parties. The effects

41 See recently, on the importance of the parties' consent to documents-only arbitration for the validity of the award, *CBS v CBP* [2021] SGCA 4.

42 See *e.g.*, *Jur* (n 26).

of such a decision on the validity of the award and on its enforceability are receiving attention in the literature, especially in the wake of the COVID-19 pandemic.[43]

Additional doubts may arise with respect to the overall duration of the arbitral procedure. As outlined in section 2, many blockchain-based mechanisms aim at expediting (or even automating) different aspects of dispute resolution, so as to enhance efficiency. However, doubts may arise as to whether a particularly fast procedure (which may last less than a week) is sufficient to afford the parties a reasonable opportunity to present their case. As already mentioned, similar concerns have been voiced with respect to the judicial enforcement of emergency arbitrator decisions, which also prioritise speed over the multiplication of opportunities for the parties to put forth their arguments and evidence.[44] It is impossible to indicate a bright-line timeframe for how long a blockchain-based arbitration procedure should last, striking an acceptable balance between speed and due process. To the contrary, the requested court will need to evaluate on a case-by-case basis whether, given the nature of the dispute and the parties' argument, the duration of the arbitration was sufficient to afford the disputants a sufficient opportunity to set forth their arguments and, if necessary, furnish proof.

4.4 *Substantive Public Policy*

In addition to procedural public policy (discussed in the previous paragraph), arbitral awards may be declined recognition and enforcement on grounds of substantive public policy (enshrined in Article V(2)(b) of the New York Convention). At first glance, these grounds for refusal seem to have little to do with the fact that the arbitral procedure made use of blockchain technologies. Indeed, substantive public policy refers to the substance of the arbitrators' determination on the merits, rather than to procedural aspects. Nevertheless, it is necessary to mention a worrisome development: blockchain-based escrow mechanisms, such as the ones described above in sub-section 2.1, are sometimes deployed by parties entering into agreements on so-called "darknet"

43 Maxi Scherer, "The Legal Framework of Remote Hearings," in Maxi Scherer, Niuscha Bassiri and Mohamed S. Abdel Wahab (eds), *International Arbitration and the COVID-19 Revolution* (Alphen aan den Rijn: Kluwer Law International 2020), 65. See also Karthik Nagarajan & James J. East Jr., "Salient Considerations for Remote International Arbitration Hearings," in Shaheeza Lalani and Steven G. Shapiro (eds), *The Impact of COVID on International Disputes* (Boston: Brill 2022).

44 See (n 30) above and accompanying text.

marketplaces.[45] These contracts may well be incompatible with the substantive public policy of the place where recognition and enforcement may theoretically be sought (*e.g.* a contract for the sale of drugs that cannot be freely sold in the place of enforcement). This incompatibility with public policy, however, is the likely reason why the parties to the transaction denominate their agreement in a cryptocurrency in the first place, and set up an escrow wallet. In other words, the parties know that any dispute resolution outcome would not be granted recognition and enforcement, even it if were to theoretically qualify as an arbitral award. Mindful of this, the parties set up a mechanism of "self-enforcement," which is supposed to ensure the implementation of the dispute resolution outcome without relying on traditional recognition and enforcement procedures (such as the ones made possible by the New York Convention). In practice, therefore, these arbitral awards will never be submitted for recognition and enforcement, especially whenever doing so may be construed as a *notitia criminis*, depending on the content of the transaction. Needless to say, the use of technology to set up private adjudication mechanisms which elude public policy and mandatory law is troublesome, and deserves close attention not only from law enforcement agencies, but also from academics.

5 The Future Potential Relevance of Blockchain Technology for Recognition and Enforcement: Distributed Ledgers for Judgments and Awards

Recognition and enforcement procedures for both court judgments and arbitral awards are still often paper-based. Just to mention some examples, Article 37(1)(a) of the Brussels I *bis* Regulation[46] requires the party seeking to rely on a judgment to produce "a copy of the judgment which satisfies the conditions

45 Farida Sabry et al., "Anonymity and Privacy in Bitcoin Escrow Trades," in *WPES'19: Proceedings of the 18th ACM Workshop on Privacy in the Electronic Society* (New York: Association for Computing Machinery 2019), 211; Steven Goldfeder et al., "Escrow protocols for cryptocurrencies: How to buy physical goods using Bitcoin," in Aggelos Kiayias (ed), *International Conference on Financial Cryptography and Data Security* (Cham: Springer 2017), 321. Martin Horton-Eddison and Matteo Di Cristofaro, "Hard Interventions and Innovation in Crypto-Drug Markets: The escrow example (Policy Brief 11)" (*Global Drug Policy Observatory*, August 2017) <https://www.swansea.ac.uk/media/Hard-Interventions-and-Innovation-in-CryptoDrug-Markets-The-escrow-example.pdf> accessed 28 June 2023.

46 Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, [2012] OJ L351/1.

necessary to establish its authenticity." Similarly, Article 13(1)(a) of the 2005 Hague Convention on Choice of Court Agreements requires the party seeking recognition or enforcement to produce, among other documents, "a complete and certified copy of the judgment." Along similar lines, as far as arbitration is concerned, Article IV(1)(a) of the New York Convention requires "the duly authenticated original award or a duly certified copy thereof."

These requirements often result in significant costs for the judgment- or award-creditor, who may occasionally even be deterred from collecting the judgment or award altogether. Blockchain technologies have been identified as a possible solution to this problem. More specifically, it would be possible to create a distributed ledger where court judgments and/or arbitral awards are immutably registered. The judgment- or award-creditor, then, would be able to seek recognition and enforcement simply by referring to a "hash," *i.e.* to a string of characters that univocally identifies the relevant title. The blockchain would automatically "verify" the award, *i.e.* confirm that the hash corresponds to a certain judgment or award. At the time of writing, no such system has been put in place yet. However, initiatives in this sense do exist: the Dubai International Financial Centre courts, for instance, have announced the intention to set up a blockchain infrastructure "to aid verification of court judgments for cross-border enforcement."[47]

For any such initiative to be successful, cooperation among different states is necessary. A blockchain-based system for the verification of court judgments and/or arbitral awards would require different states to agree on how the peer-to-peer network should be set up, and how the relevant documents (court judgments, arbitral awards, or both) should be registered. In the presence of such a technological infrastructure, then, the domestic law governing the recognition and enforcement of judgments and/or award should be amended, so as to dispense with the requirement for the party seeking enforcement to produce originals or certified copies, whenever the judgment or award is registered on the distributed ledger. Moreover, were such a system to be available for arbitration, further obstacles would exist, as the state will obviously not automatically receive a copy of all awards issued by tribunals seated in its territory. Thus, new provisions of domestic law would likely be necessary to enable the award creditor (or a different entity, such as an arbitral institution) to deposit the original or a certified copy of the award with a competent authority at the seat of arbitration. This authority, in turn, would proceed to register the award on the blockchain, thus facilitating recognition and enforcement in jurisdictions

47 Dubai International Financial Centre, "Courts of the Blockchain" (*DIFC*) <http://www.courtsofthefuture.org/#courts-of-blockchain> accessed 28 June 2023.

other than the seat. These other jurisdictions, of course, would also need to agree to the use of the distributed ledger. Thus, the creation of such a mechanism would entail significant burdens both in terms of legal reform at the domestic level, and from the point of view of practical implementation.

In the absence of any amendment to the international framework governing the recognition and enforcement of judgments and/or award, the viability of such a blockchain-based system would mainly rely on more-favourable-treatment clauses. By way of example, under Article VII(1) of the New York Convention, award creditors remain free to seek recognition and enforcement under a domestic regime that may impose less demanding requirements than the ones set forth in the Convention. Therefore, the award creditor may seek recognition and enforcement of an award by communicating a hash, in accordance to national provisions of law enabling him/her to do so instead of supplying an original award or certified copy pursuant to Article IV(1)(a) of the New York Convention. Obviously, such a system would be entirely reliant on the states' willingness to accord a more favourable treatment, in the absence of any international obligation in this sense. The only theoretical alternative would be a new instrument, imposing an international obligation on the contracting states to accord recognition and enforcement of judgments and/or award when the judgment- or award-creditor produces a hash enabling the verification of the relevant title.

6 Conclusions

This chapter has analysed the interplay between blockchain technologies and dispute resolution outcomes. Over the past decade, blockchain technologies have enabled the development of a diverse range of dispute resolution mechanisms. While some of them resemble in some ways previously existing mechanisms (such as arbitration), others constitute entirely novel models of dispute resolution, which aim to ensure the automatic implementation of the outcome on the blockchain, rather than relying on traditional recognition and enforcement procedures. For this reason, the question as to whether blockchain-based dispute resolution outcomes may be recognised and enforced cannot be answered in general terms. To the contrary, different blockchain-based procedures call for different legal qualifications, depending on their specific features. As a consequence, some dispute resolution outcomes may be able to produce "on-chain" effects, but do not enable the prevailing party to seek recognition and enforcement. By contrast, other dispute resolution mechanisms may qualify as arbitration, thus in principle leading to outcomes enforceable

inter alia under the 1958 New York Convention. For this latter category of procedures, recognition and enforcement are in principle possible, but it may be possible to invoke one or more grounds for refusal, depending on the characteristics of the procedure, and the way in which the tribunal carried it out.

As far as court judgments are concerned, no national legal system to date has integrated its courts with blockchain technologies in such a way as to facilitate (or even automate) the recognition and enforcement of judgments. This chapter has outlined the obstacles that any such attempt would face, assessing its feasibility in light of the current international framework enabling recognition and enforcement of judgments and awards.

In conclusion, blockchain technologies interact with recognition and enforcement procedures in different ways. On the one hand, blockchain technologies bring about a degree of automation that may, to a certain extent, make traditional recognition and enforcement procedures obsolete. However, this chapter argues that recognition and enforcement procedures are likely to remain of crucial importance in a wide range of scenarios, where the technology is not sufficient to ensure the implementation of dispute resolution outcomes "on-chain", and more generally to produce the effects (*e.g. res judicata*) that a party may wish to rely upon. For this reason, in the future, blockchain technologies may come to interact with recognition and enforcement procedures in a less competitive fashion, with the former not attempting to render the latter obsolete, but rather facilitating the swift settlement of disputes and the efficient cross-border circulation of judgments and awards. The road towards the practical implementation of such systems, however, remains fraught with uncertainty.

PART 5

National Reports

∴

CHAPTER 22

Conflict of Laws and Tokens in Swiss Private International Law

Pascal Favrod-Coune and Kévin Belet

1 Introduction

In several jurisdictions, legislators and regulators have become increasingly interested in the potential of distributed ledger technologies (DLTs). Diverse approaches have been followed and some countries have adopted new legal provisions catered to these technologies. In this respect, Switzerland figures among one of the first jurisdictions to include DLTs in its legal framework through the recently adopted act commonly referred to as the "DLT Act." This Act is not a specific federal act in itself but is an act structured as a framework that amends ten federal acts already into force in various areas of laws (private law, financial regulation, debt enforcement and bankruptcy, *etc.*).

A major difficulty with regulating and enacting rules applicable to DLTs is that such technologies are, by nature, not limited by state borders. It is complicated, if not impossible, to determine the place where a token is issued or located as it materially constitutes only a piece of information stored on a blockchain. This may create difficulties when attempting to determine the law governing the token, or the competent jurisdiction when a conflict arises. This issue needed to be addressed by Swiss lawmakers, as the DLT Act logically only applies when Swiss law is applicable.[1] Adopting conflict-of-laws rules that apply to tokens were accordingly necessary. This is why the Private International Law Act (PILA)[2] has also been amended to include DLTs.

The objective of this chapter is to present the Swiss Private International Law (PIL) applicable to tokens. We will first describe the notion of tokens (2) by detailing how they may be classified. In this regard, we will present two

1 Swiss Federal Council report, "Legal framework for distributed ledger technology and blockchain in Switzerland: An overview with a focus on the financial sector" (*Federal Council*, 14 December 2018), 70 <https://www.newsd.admin.ch/newsd/message/attachments/55153.pdf> accessed 19 March 2023.

2 Federal Act on Private International Law (PILA) of 18 December 1987, AS 1988 1776, SR 291 ("PILA").

© PASCAL FAVROD-COUNE AND KÉVIN BELET, 2023 | DOI:10.1163/9789004514850_024
This is an open access chapter distributed under the terms of the CC BY-NC-ND 4.0 license.

taxonomies of tokens: firstly from a technical perspective, and secondly from a legal perspective based on financial regulation and private law. The amendments of the PILA in the context of the DLT Act will then be studied in detail (3). We will explain the genesis and the general objectives of the DLT Act as well as the legislative process that led to its adoption. We will then turn to the new provisions of the PILA that entered into force on 1 February 2021, and distinguish between general principles to determine the applicable law to tokens, and the exception when pledging a token. We will also provide a critical appraisal of the amendments of the PILA. The last section consists of concluding remarks (4).

2 Notion of Tokens

Before thoroughly examining the Swiss PIL applicable to tokens, it is useful to describe what a token effectively represents. In this respect, we will first outline how tokens are perceived from a technical and legal viewpoint, even though no definition is generally accepted among scholars (2.1). A taxonomy of tokens is nevertheless useful to classify existing types of tokens, both from a functional and legal standpoint (2.2).

2.1 *Description of Tokens*

Since the emergence of DLTs and the publication of the white paper introducing the well-known Bitcoin in 2008, a great number of different types of tokens have been created. Those cover a large – and still increasing – area of applications.

From a technical point of view, a token can be described as a cryptographic representation of an asset or access rights, stored on an underlying blockchain.[3] Accordingly, a token solely represents units of digital information.[4] Usually, a

3 Benjamin V. Enz, "Die zivilrechtliche Einordnung von Zahlungs-Token wie dem Bitcoin als «Registerwertdaten» und deren Aussonderbarkeit im Konkurs de lege lata und de lege ferenda" (2020) 9 Schweizerische Juristen-Zeitung 291, 292; Vaïk Müller and Vincent Mignon, "La qualification juridique des tokens: aspects réglementaires" (2017) 4 Gesellschafts- und Kapitalmarktrecht 486, 488.

4 Mirjam Eggen, "Was ist ein Token?" (2018) 5 Aktuelle Juristische Praxis 558, 589; Enz (n 3), 292; Benjamin V. Enz, "Kryptowährungen im Lichte von Geldrecht und Konkursaussonderung" (PhD diss., University of Zurich, 2019), 43; Andreas Furrer et al., "Die Rechtswirkung algorithmisch abgewickelter DLT-Transaktionen: Von der Notwendigkeit der funktionalen Kategorisierung eines Blockchain-Tokens und dessen Synchronisation mit der angestrebten Rechtswirkung" (*Jusletter*, 26 November 2018), N 2 <https://jusletter.weblaw.ch/fr/dam

token can be used or transferred by applying the principle of asymmetric cryptography, which is a system that uses pairs of keys: a public key that is known to others than the holder of the token, and a private key, which is personal and should never be known by anyone except the owner.[5]

From an economic standpoint, tokens can be used as means of payment and are, in this sense, comparable to some extent to foreign currencies (therefore the term "cryptocurrencies").[6] They can also provide a right of access to a service (for example the holder of a STORJ token can buy storage for files on a decentralised network),[7] or serve as an investment or a store of value, with a right to a form of dividend (some protocols, for example MultiversX, offer other tokens to holders of one of their tokens).[8] In contrast to fiat currencies, cryptocurrencies are not issued centrally, but through a network involving different nodes (so-called peer-to-peer network). The macroeconomic trend of cryptocurrencies is quickly growing, and the total capitalization of cryptocurrencies in 2021 exceeded the threshold of USD 2000 billion.[9]

From a legal perspective, commentators describe a token as a digital representation of a right (*e.g.* a claim or a corporate right) or a single unit of account recorded in a register (database) by means of DLT such as a blockchain or similar technological means.[10] Yet, despite the growing understanding of the

---

/publicationsystem/articles/jusletter/2018/959/anforderungen-an-die_f813e868d9/Jusletter_anforderungen-an-die_f813e868d9_fr.pdf>, accessed 19 March 2023; Markus F. Huber, Silvan Guler, and Janine Dumont, "By the same token" (2018) 4 Steuer Revue 292, 294; Müller and Mignon (n 3).

5 Pascal Favrod-Coune, "The Patent-Eligibility of Blockchains in Europe and the United States" (2019) 2 ex ante 32, 38; Martin Hess and Patrick Spielmann, "Cryptocurrencies, Blockchain, Handelsplätze & Co," in Thomas U. Reutter and Thomas Werlen (eds), *Kapitalmarkt – Recht und Transaktionen XII* (Zurich: Schulthess 2017), 157; Vincent Mignon, "Le «[B]itcoin», un nouveau défi pour le juriste suisse ?" (*Jusletter*, 4 May 2015), N 14 <https://jusletter.weblaw.ch/fr/juslissues/2015/800/le----b-itcoin--%2c-un_29437b5cea.html> accessed 19 March 2023.

6 Huber, Guler and Dumont (n 4), 294.

7 See Ben Golub, "An Overview of Tokens Uses, Flows and Policies at Storj Labs" (*STORJ*, 5 December 2018) <https://www.storj.io/blog/an-overview-of-tokens-uses-flows-and-policies-at-storj-labs> accessed 19 March 2023.

8 This is the case of MultiversX, which pays the holders of their EGLD tokens in MEX. See, in particular, Benjamin Mincu, "The Maiar exchange and MEX token: Snapshots and Claiming" (*MultiversX*, 19 April 2021) <https://multiversx.com/blog/maiar-exchange-mex-distribution/>.

9 Total capitalisation as of May 2021. CoinMarketCap, "Global Cryptocurrency Charts: Total Cryptocurrecy Market Cap" (*CoinMarketCap*) <https://coinmarketcap.com/charts/> accessed 19 March 2023. Bitcoin alone accounts for half of the total capitalisation.

10 Fedor Poskriakov, "Conservation et négoce de cryptoactifs – aspects choisis du droit des marchés financiers," in Alexandre Richa and Damiano Canapa (eds), *Droit et économie numérique* (Stämpfli 2021), 84: "représentation numérique d'un droit (e.g., créance ou

notion of tokens, there is no commonly accepted classification nor a general definition, particularly in Swiss law.[11]

The tokens' ecosystem is vast and continuously expanding. Indeed, in addition to approximately ten thousand types of tokens that exist, there are also a growing number of protocols or decentralised applications (DApps), such as Binance Smart Chain,[12] MultiversX[13] or Tokenmint,[14] which allow anyone to conveniently create new types of tokens. Some networks permit active participation to the holders of their tokens (for example, the Kleros arbitration protocol allows its holders to be arbitrators in a dispute on the blockchain and to be remunerated in PNK[15] for their participation in arbitration proceedings).[16] Due to their multi-faceted aspects, tokens have a vast range of applications. In this respect, it is nearly impossible to consider all the possibilities and functions that they will offer in the future, especially regarding the progress made over the last decade.

2.2 *Taxonomy of Tokens*

The following section will firstly attempt to classify tokens according to their functions from a technical point of view (2.2.1). We will then classify tokens from a Swiss legal perspective (2.2.2). In this context, different classifications

droits sociaux) ou d'une simple unité de compte inscrite sur un registre (base de données) au moyen de la technologie des registres distribués (TRD) comme par exemple une chaîne de blocs (blockchain) ou un moyen technologique analogue.»

11 Enz (n 4), 44; Frédéric Ney, "Le traitement fiscal lié à l'émission de jetons d'utilité et de jetons d'investissement au moyen de la technologie « blockchain »" (2020) 76 Revue de droit administratif et de droit fiscal II 135, 138; Dominic Wyss, "Initial Coin Offerings (ICOs) – Ein Diskussionsbeitrag" (*Jusletter*, 3 December 2018), N 12 <https://jusletter.weblaw.ch/juslissues/2018/960/initial-coin-offerin_db01b2f3ff.html> accessed 19 March 2023.

12 Cointool, "Create Token" (*Cointool*) <https://cointool.app/bnb/bsccreateToken> accessed 19 March 2023.

13 MultiversX, "The Internet Scale Blockchain is Live!" (*multiversX*) <https://multiversx.com/> accessed 19 March 2023.

14 <https://tokenmint.net/> accessed 19 March 2023.

15 The PNK is the token from the Kleros DApp.

16 Pascal Favrod-Coune and Kévin Belet, "La convention d'arbitrage dans un smart contract" (2018) 9 Aktuelle Juristische Praxis 1105, 1116–17; Rolf H. Weber and Okan Yildiz, "Alternative Dispute Resolution auf DLT-Handelsplattformen" (*Jusletter*, 14 June 2021), N 35 <https://jusletter.weblaw.ch/juslissues/2021/1070/alternative-dispute-_86bf26769b.html> accessed 19 March 2023. For more information on the Kleros project, see in particular Favrod-Coune and Belet (n 16) and the Kleros protocol white paper: Clément Lesaege, Federico Ast and William George, "Kleros: Short Paper v1.0.7" (*Kleros*, September 2019) <https://kleros.io/assets/whitepaper.pdf> accessed 19 March 2023.

can be made according to the area of law that the analysis targets.[17] In Swiss legal literature, commentators tend to focus on the classification for a financial regulation analysis because the regulatory treatment of a token is of primary importance prior to issuing one. Therefore we will briefly present such classification before focusing on a private law classification, as this methodology is equally valid for a PIL analysis.

2.2.1 Functional Taxonomy

The following differences are relevant when determining the functional classification of tokens:

– Native tokens and non-native tokens (*infra* 2.2.1.1);
– Protocol tokens and application tokens (*infra* 2.2.1.2);
– Fungible tokens and non-fungible tokens (*infra* 2.2.1.3).

2.2.1.1 *Native Tokens and Non-Native Tokens*

Native tokens ("intrinsic tokens" or "built-in tokens") are to be distinguished from non-native tokens ("asset-backed tokens").[18] This distinction resides primarily from where the value of the token derives. On the one hand, a native token takes its value solely from its representation on the blockchain (on-chain). On the other hand, a non-native token is valued not only on the basis of its representation on the blockchain, but also on its represented value outside of it (off-chain).[19]

Native tokens are any conceptual representation of a value that is uniquely composed by the existence and operation of a decentralised protocol or decentralised application.[20] In this regard they can, for instance, represent a cryptocurrency,[21] be used to access features and applications,[22] confer voting rights in a decentralised autonomous organization (DAOs)[23] or combine several of

17 Poskriakov (n 10).
18 Müller and Mignon (n 3), 487.
19 Ney (n 11), 140. See Adan, "Taxonomy blockchain-based crypto-assets" (*Adan*, 8 April 2021) <https://adan.eu/en/article/taxonomy-blockchain-basedcrypto-assets-en> accessed 19 March 2023.
20 Adan (n 19).
21 This is the case for Bitcoin, Bitcoin Cash, Litecoin and Monero.
22 This is the case for the CRO of the crypto.com DApp that offers an increasing range of features depending on the number of CROs held; see Crypto, "The World's Fastest Growing Crypto App" (*Crypto*) <https://crypto.com/> accessed 19 March 2023.
23 For example, the BitShares DAO that allows holders of the BTS token to elect decision-makers and validators of blocks, see BitShares, "Our mission is to provide Decentralized Software solutions to any KIND of centralized problems in every INDUSTRY" (*BitShares*) <https://bitshares.org/> accessed 19 March 2023.

these characteristics.[24] These tokens have no link with other objects or assets which are not native tokens.[25] Thus, their value derives directly from the information inscribed on the blockchain itself. Such value will increase according to the demand for the application linked to it.[26]

The control of native tokens is exclusively done "on-chain." The person who knows or controls the private key holds the token and is the only one able to use it. A parallel may be made with the law applicable to rights *in rem* in Switzerland, where possession establishes a presumption of ownership. This principle dates back to Roman law[27] and is followed in several other jurisdictions.[28] Thus, as with physical goods, the holder of the token can benefit from it.

Unlike native tokens, non-native tokens (or "tokenised assets") partly derive their value from outside the blockchain.[29] They represent, at least in part, an underlying asset.[30] This may be fiat currencies,[31] commodities,[32] or any other existing financial instruments. Even though developments in this respect mainly concern the financial markets, non-native tokens can be useful in areas other than finance. For instance, non-native tokens can represent any physical asset, such as works of art (physical or digital). In principle, it is possible to tokenise any kind of asset, such as plane tickets, books, songs, or shares of a company.

Non-native tokens raise several legal issues regarding the distinction between the token and the underlying asset. The holder of the private key can freely exploit the token on-chain. However, the underlying asset does not

24 This is the case for the CHSB, which allows its holders to benefit from low fees on the platform and to have a voice in the DAO of the SwissBorg application, SwissBorg, "The SwissBorg Token (CHSB)" (*SwissBorg*) <https://swissborg.com/buy-chsb> accessed 19 March 2023.

25 Adan (n 19).

26 For example, the CRO or the CHSB gain value solely on the usage of their respective application and services.

27 Pascal Pichonnaz, "Commentaire de l'art. 930 CC," in Pascal Pichonnnaz, Bénédict Foëx, and Denis Piotet (eds), *Commentaire romand Code civil II. Art. 457–977 CC. Art. 1–61 Tit. Fin. CC* (Basel: Helbing Lichtenhahn 2016); Pascal Pichonnaz, *Les fondements romains du droit privé* (Geneva, Zurich, Basel: Schulthess 2020), 255.

28 See Ernst Wolfgang, "Vorbermerkungen zu Art. 930–937," in Thomas Geiser and Stephan Wolf (eds), *Basler Kommentar Zivilgesetzbuch II* (Basel: Helbing Lichtenhahn 2019), N 6 et seq.

29 Adan (n 19).

30 Pascal Favrod-Coune, "Crowdfunding. Analyse de droit suisse du financement participatif" (PhD diss., University of Lausanne, 2018), 49.

31 For example, stablecoins that are tied to the US dollar, such as USDC, USDT or BUSD.

32 For example, commodities that are tied to gold, such as PAX Gold.

necessarily belong to him, so that he cannot use it. This is particularly the case with tokenised shares where the token's acquisition does not attribute ownership of the underlying share. However, the tokenisation of assets in the form of non-native tokens have a functional, added value to the asset.[33] They allow assets to be represented on a blockchain, therefore making them benefit from the advantages of DLT, such as efficiency of transactions and programmability through smart contracts.[34]

It results from the above that the distinction between native and non-native tokens is useful to determine whether the token is intrinsically linked to the blockchain.[35] Native tokens do not refer to any exterior value while non-native tokens' values and rights depend on elements outside the blockchain.

2.2.1.2 *Protocol Tokens and Application Tokens*

A second technical distinction exists between protocol and application tokens. The first allows a blockchain to function[36] (for example BTC, ETH, BNB, DOT),[37] while the latter makes it possible for DApp to function on an existing protocol (for example AAVE, PANCAKESWAP or POLKAMARKETS).[38] As a result, protocol tokens are those on which application tokens rely on to run their DApp.

Protocol tokens refer to the set of rules that enables consensus to be reached on the network and make it functional.[39] Initially, the first DLTs were based on the proof-of-work principle, whereas the most recent ones use the proof-of-stake principle.[40] However, a decision to change the protocol of a specific blockchain cannot be taken unilaterally but can only be the result of consensus between operators and users.[41] Thus, protocol tokens are necessary for a

33 Adan (n 19).

34 *Id.*

35 Whether to the protocol or to a decentralised application.

36 Federal Council report (n 1), 34.

37 These are the native tokens of the Ethereum, Binance Smart Chain and Polkadot protocols, respectively.

38 AAVE is an application token of the Ethereum protocol, Pancakeswap is such a token of the Binance Smart Chain protocol, and Polkamarkets is the same for the Polkadot protocol.

39 Adan (n 19).

40 An increasing number of blockchains are moving their protocols to the more efficient proof-of-stake mechanism. This is for example the case for the Ethereum blockchain, which will implement the proof-of-stake protocol. Corwin Smith, "Proof-of-Stake (POS)" (*Ethereum*, 23 May 2022) <https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/> accessed 19 March 2023.

41 Adan (n 19).

blockchain to correctly function,[42] notably by allowing consensus between validators. They accordingly play a structural role in the ecosystem.

Conversely, application tokens are the result of functionality added to the protocol and allow concrete uses of the blockchain for users. They simply enable an application to run, which is itself deployed on a protocol that is validated by protocol tokens. Applications constitute another layer built on the main protocol.[43] The application tokens are registered on the underlying blockchain even though this is not necessary for its basic functions. For example, ERC20, used for fungible tokens, and ERC721, used for non-fungible tokens,[44] are the references for token applications on the Ethereum blockchain.

A major interest of DLT is that it allows the development of different applications. These various DApps are functional because of application tokens. Currently, most projects focus on decentralised finance (so-called DeFi) and some applications already allow to raise funds through crowdfunding,[45] to acquire cryptocurrencies,[46] to provide cash in exchange for other tokens[47] or simply to lend or borrow tokens.[48] However, it is conceivable that over time a growing number of areas could be covered by such applications. While some applications increase smart contracts' efficiency or are useful to their proper functioning (for example, oracles provide data from external systems that are needed by smart contracts to be executed),[49] some others offer the possibility to make bets,[50] to participate in auctions,[51] to acquire non-fungible

42 Ney (n 11), 140.

43 *Id.*; Federal Council report (n 1), 34.

44 On the distinction between fungible and non-fungible tokens, see *infra* sec. 2.2.1.3.

45 DAO Maker is one of the oldest DApp to raise funds through a blockchain. DAO Maker, "Venture Capital Re-created for the Masses" (*DAO Maker*) <https://daomaker.com/> accessed 19 March 2023.

46 For example SwissBorg and Crypto.com via their smartphone application. SwissBorg, "Invest in cryptos the smart way" (*SwissBorg*) <https://swissborg.com/fr/> accessed 19 March 2023 and Crypto (n 22), respectively, or the DApp Uniswap. Uniswap, "Uniswap Protocol" (*Uniswap*) <https://uniswap.org/> accessed 19 March 2023.

47 Pancakeswap, "Pancakeswap" (*Pancakeswap*) <https://pancakeswap.finance/> accessed 19 March 2023.

48 AAVE, "AAVE Liquidity Protocol" (*AAVE*) <https://aave.com/> accessed 19 March 2023.

49 See TEEX, "What are Oracles? Smart Contracts, & 'The Oracle Problem'," (*Medium*, 20 August 2019) <https://medium.com/@teexofficial/what-are-oracles-smart-contracts-the-oracle-problem-911f16821b53> accessed 19 March 2023; Chainlink, "Chainlink" (*Chainlink*) <https://chain.link/> accessed 19 March 2023.

50 Polkamarket, "Autonomous Prediction Market Protocol" (*Polkamarkets*) <https://www.polkamarkets.com/> accessed 19 March 2023.

51 KSM, "Parachains Are Here" (*Kusama Network*) <https://kusama.network/> accessed 19 March 2023.

tokens[52] or to collect sports cards.[53] Protocols frequently provide platforms for deploying applications and ultimately issuing new tokens.[54]

In a way, application tokens are "second-class citizens",[55] as they invariably depend on the protocol on which they are deployed. This is evidenced by the fact that transaction fees (called gas on the Ethereum blockchain) for these applications are paid with protocol tokens.

2.2.1.3 *Fungible and Non-fungible Tokens*

The last distinction is the tokens' fungibility. Tokens that are unique and those that have similar characteristics and qualities are to be differentiated. Indeed, when a person buys a fungible token, he chooses the quantity that he wants to purchase, for example one bitcoin or one ether. It does not matter whether the token was mined several years ago or only very recently. Conversely, non-fungible tokens represent unique pieces that must be distinguished from other tokens of the same kind.

Fungible tokens are equivalent and interchangeable with each other. Therefore, they can be divided into fractions[56] and combined in the same way as fiat currencies. Fungible tokens are the most common form: they can constitute native and protocol tokens like bitcoins or ethers. However, they can also take the form of application tokens such as AAVE or Uniswap.

Non-fungible tokens (commonly referred to as NFTs) are not equivalent or interchangeable.[57] They represent rights to physical or digital assets. An NFT can, for instance, represent a painting[58] (whether physical or digital), or physical goods such as watches or collectibles.[59]

---

52 OpenSea, "Discover, collect, and sell extraordinary NFTs" (*OpenSea*) <https://opensea.io/> accessed 19 March 2023.

53 Sorare, "Global Fantasy football" (*Sorare*) <https://sorare.com/> accessed 19 March 2023.

54 Adan (n 19).

55 *Id.*

56 For example, one bitcoin can be divided into fractions of 100000000. This fraction of a bitcoin, 0.00000001 bitcoin, has a name: a Satoshi. This name refers to Satoshi Nakamoto, the pseudonym of the person or persons who developed Bitcoin.

57 Adan (n 19).

58 Recently, the highest sale of an NFT by Sotheby's reached US $17 million. Sotheby's, "$17 Million Realized in Sotheby's First NFT Sale with Digital Creator Pak" (*Sotheby's*, 16 April 2021) <https://www.sothebys.com/en/articles/17-million-realized-in-sothebys-first-nft-sale-with-digital-creator-pak> accessed 19 March 2023.

59 Sorare allows to acquire and collect footballer cards in the form of NFTs and trade them. Sorare (n 53).

2.2.2 Taxonomy in Swiss Law

From a legal viewpoint, tokens need to be categorised to link rights and obligations to them, or simply to be legally categorised. In Swiss legal literature, different categorisations exist that rely on the field of law in question in order to determine the applicable legal framework. In particular, the classification used in financial regulation is not identical as the one used in private law.[60]

2.2.2.1 *In Financial Regulation*

To solve the issues raised by cryptocurrency fundraising (Initial Coin Offerings or ICOs), FINMA has decided to address the thorny issue of the legal classification of tokens.[61] Having prepared it in February 2018, FINMA is the first Swiss authority to provide a taxonomy of tokens to determine the applicable financial regulation.[62]

To do so, FINMA has published guidelines in which it establishes three categories based on the underlying economic function of tokens:[63]

- Payment tokens: such tokens constitute cryptocurrencies. They are accepted as a means of payment for obtaining goods or services.[64] Their purpose is to transfer funds or values. This class of tokens does not confer any rights against the issuer.[65] For instance, Bitcoin is a payment token.[66]
- Utility tokens: they allow access to and use of the functionalities of a DApp or to obtain a service.[67] Voucher, fidelity points (for example miles for an airline company) could thus be embedded in utility tokens.[68]
- Asset tokens: those include tokens representing assets ("asset-backed token").[69] They may, in particular, represent debt or equity,[70] a share

60 Federal Council report (n 1), 46.

61 FINMA, "Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs) Published 16 February 2018" (*FINMA*, 16 February 2018) <https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung> accessed 19 March 2023.

62 See Tarek Houdrouge and Jérémie Tenot, "Le droit suisse à l'heure de la technologie des registres électroniques distribués" (2020) 2 not@lex 49, 51.

63 FINMA (n 61), 1 et seq.; Poskriakov (n 10), 85.

64 Poskriakov (n 10), 86.

65 *Id.*, 83; Federal Council report (n 1), 46; FINMA (n 61), 3; Ney (n 11).

66 Huber, Guler, and Dumont (n 4), 294–95.

67 Ney (n 11), 138–39; Poskriakov (n 10), 88.

68 Poskriakov (n 10), 88.

69 FINMA (n 61), 3.

70 *Id.*

in future company earnings[71] or a right to the payment of dividends or interests,[72] but can also represent other types of assets.[73] Asset tokens could constitute securities (*valeurs mobilières* or *Effekten*) pursuant to art. 2 lit. b Financial Market Infrastructure Act,[74] at least when the economical function is relevant for capital markets.[75]

In the guidelines, FINMA clarifies that the different categories are not mutually exclusive. This means that a token can fall into several categories at the same time (so-called "hybrid tokens").[76] For example, an asset token can also be considered as a payment token.[77] Consequently, it will be considered both as a security and as a means of payment. Sometimes, utility tokens will be accepted as means of payment and referred to as hybrid tokens.[78]

FINMA is competent to verify that financial regulation is respected and does not deal with other rules that may be applicable to tokens, in particular in private law (including PIL) or tax law. In its Guidelines regarding ICOs, FINMA makes clear that it "treats enquiries exclusively from the perspective of existing financial market regulation. Market participants themselves remain responsible for evaluating and complying with other obligations especially under civil law and tax law."[79] As a result, this taxonomy is relevant to assess the applicable financial regulation but may not be appropriate to determine the application of other rules, notably in PIL. In this respect, we argue that another taxonomy is needed.

2.2.2.2 *In Private International Law*

As already seen above, the qualification of tokens should be distinguished depending on the area of law at hand. The economic approach used by FINMA is not suitable to determine the applicable rules because in PIL such rules will depend on the function and the rights that the token embeds. Based on another

71 *Id.*
72 Federal Council report (n 1), 46.
73 Ney (n 11), 139.
74 Federal Act on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading (Financial Market Infrastructure Act, FinMIA) of 19 June 2015, AS 2015 5339, SR 958.1 ("SR 958.1").
75 Poskriakov (n 10), 87.
76 Nicolas Rouiller, *Cryptocurrencies: current realities, philosophical principle and legal mechanism* (EurAsian Scientific Editions Ltd, 2020), 12.
77 Ney (n 11), 134.
78 Poskriakov (n 10), 89.
79 FINMA (n 61), 3.

approach, the Federal Council classified tokens in four different categories in its report published on 14 December 2018.[80] Those categories are:
– tokens linked to a claim;
– tokens linked to a membership;
– tokens linked to a right *in rem*;
– cryptocurrencies.

The tokens falling under these categories are treated differently under private law because they embed rights that are subject to distinct provisions. The rules applying to tokens linked to a claim depend on the underlying contract, whereas tokens linked to a membership are subject to company law and tokens linked to a right *in rem* are subject to the provisions applying to such rights. The categories in conflict-of-laws rules set forth in the PILA are based on those in substantive law. This law indeed provides for different conflict-of-laws rules for different areas of law, for example contract law (Chapter 9 of the PILA), company law (Chapter 10 of the PILA) or rights *in rem* (Chapter 7 of the PILA).

For tokens linked to a claim (*créance* or *Forderung*), the law applicable to the contract should also be applied to the token in accordance with the *lex contractus* where the claim arises from a contract.[81] Under Swiss law, a claim can be defined as a subjective right to request positive or negative behaviour from a specific person – the debtor.[82] In most cases, the right acquired with a token is a claim against the issuer. This claim is embedded in the token and, according to the intention of the parties, can be asserted through the token.[83] The starting point for the analysis is therefore freedom of contract, which places great importance on the will of the parties and in the qualification of the contract. For that purpose, the name chosen by the party does not matter and it is necessary to look at the real and common intention of the parties.[84]

The contractual aspects of tokens may combine several features of contracts known under Swiss law or incorporate new types of contracts (innominate contracts). They can also combine elements of different types of contracts.[85] If the token gives the right to obtain a loan or to the exchange against another token, it could be classified as a loan contract pursuant to art. 312 *et seq.* of the

80 Federal Council report (n 1), 71.
81 *Id.*, 74.
82 "La créance est un droit subjectif permettant d'exiger un comportement positif ou négatif (une prestation) d'une personne déterminée ou de plusieurs personnes déterminées – le ou les débiteurs." Paul Piotet, *Transferts de propriété, expectatives réelles et substitutions fidéicommissaires* (Stämpfli 1992), 48.
83 Federal Council report (n 1), 46.
84 *Id.*, 47.
85 *Id.*

Code of Obligations (CO)[86] or a contract of exchange pursuant to art. 238 *et seq.* of the CO. Therefore, the type of claim represented by the token is subject to the law defined by art. 116 *et seq*. of the PILA.

When tokens are linked to a membership right (*droits sociaux* or *Mitgliedschaft*), one must look into the provisions of the PILA regarding company law. In this respect, according to art. 154 para. 1 of the PILA, the corporate rights fall under the law of where the company is incorporated (*lex societatis*).[87] In that regard, the feasibility of incorporating the corporate rights into the token is also a matter of company law.[88] It is noteworthy that, unlike contract law, company law encompasses a *numerus clausus* of company forms.[89] As long as mandatory provisions of corporate and contract law are respected, Swiss law allows to embed a membership in a company into a token.[90] With the entry into force of art. 973d *et seq.* of the CO and art. 622 para. 1 of the CO as amended by the DLT Act,[91] it is possible to transfer this membership in a company by transferring the tokens issued as ledger-based securities (*droits-valeurs inscrits* or *Registerwertrechte*).

Tokens linked to a right *in rem* (*droit réels* or *dingliche Rechte*) are, under Swiss law, absolute rights and can be asserted against anyone (*erga omnes*).[92] As with company law, there is a *numerus clausus* of rights *in rem* provided by law. The law applicable to tokens linked to a right *in rem* is, in principle, the law where the property is located pursuant to art. 99 *et seq.* of the PILA. It is this law that is relevant to determine whether it is possible to associate a right *in rem* to a token.[93]

---

86 Federal Act on the Amendment of the Swiss Civil Code (Part Five: The Code of Obligations) of 30 March 1911, AS 27 317, SR 220 ("SR 220").

87 Federal Council report (n 1), 75.

88 In this sense, Stefan Eberhard and Andreas von Planta, "Art. 155," in Pascal Grolimund, Leander D. Loacker, and Anton K. Schnyder (eds), *Basler Kommentar Internationales Privatrecht* (Helbing Lichtenhahn 2020), N 13; Florence Guillaume, "art. 155," in Andreas Bucher (ed), *Commentaire romand. Loi fédérale sur le droit international privé* (LDIP)/*Convention de Lugano* (CL) (Helbing Lichtenhahn 2011), N 20.

89 *Cf.* Arthur Meier-Hayoz, Peter Forstmoser, and Rolf Sethe, *Schweizerisches Gesellschaftsrecht. Mit neuem Firmen- und künftigem Handelsregistrerrecht und unter Einbezug der Aktienrechtsreform* (Stämpfli 2018), 349–50.

90 Federal Council report (n 1), 48.

91 On the DLT Act, see *infra* sec. 3.1.

92 Bénédict Foëx, "Introduction aux articles 641–645 CC," in Pascal Pichonnnaz, Bénédict Foëx, and Denis Piotet (eds), *Commentaire romand Code civil II. Art. 457–977CC. Art. 1–61 Tit. Fin. CC* (Helbing Lichtenhahn 2016), N 5.

93 Federal Council report (n 1), 75.

Regarding cryptocurrencies, these tokens are accepted as a means of payment, whether for the purchase of goods or of services. It is still debated among commentators what cryptocurrencies constitute under Swiss law, but most scholars classify them as intangible assets.[94] This category of tokens does not generally confer any claims against an issuer.[95] For the purpose of conflict of laws, cryptocurrencies cannot be considered as a currency pursuant to art. 147 para. 1 of the PILA, so they do not fall under the scope of this provision.[96] As a result of not being a currency, transactions paid with cryptocurrencies could be considered as a form of barter, so cryptocurrency is used as a good exchanged for another one or for a service. In this instance, conflict-of-laws rules governing contracts (art. 116 *et seq.* of the PILA) apply and the parties to the exchange can, in principle, choose the applicable law (art. 116 para. 1 of the PILA). Absent a choice of law, the law applicable is the one of the state that has the closest connection to the contract (art. 117 para. 1 of the PILA).[97] Alternatively, cryptocurrencies could also be considered as a form of private tender, in which case a cryptocurrency could be used to pay a monetary debt. In this situation, art. 147 para. 3 of the PILA provides that the law applicable at the place where the payment must be made determines whether it can be validly effected using a given currency (or cryptocurrency).[98]

In its report of December 2018, the Federal Council extensively examined the Swiss PIL issues (applicable law, courts jurisdiction as well as recognition of foreign judgments) with regard to DLT. It concluded the following:

> The legal issues arising under private international law in connection with the issue or reselling of tokens can largely be satisfactorily subsumed under the existing provisions of the PILA. Significant legal uncertainty exists solely with regard to the question of the law applicable to the transfer of tokenised claims. Legislative clarification in the form of a supplementary provision in the PILA appears called for in this regard.

94 Federal Council report (n 1), 51; Eggen (n 4), 562–563; Sébastien Gobat, "Les monnaies virtuelles à l'épreuve de la LP" (2016) 8 Aktuelle Juristische Praxis 1095, 1098–1099.

95 Federal Council report (n 1), 46.

96 Federal Council report (n 1), 77; Felix Dasser, "Art. 147" in Pascal Grolimund, Leander D. Loacker, and Anton K. Schnyder (eds), *Basler Kommentar Internationales Privatrecht* (Helbing Lichtenhahn 2020), N 10; Enz (n 4), 143.

97 See Rashid Bahar, "Conflicts of Laws on the Distributed Ledger and Negotiable Instruments" (2020) 1 CapLaw 17, 21; Barbara Graham-Siegenthaler and Andreas Furrer, "The Position of Blockchain Technology and Bitcoin in Swiss Law" (*Jusletter*, 8 May 2017), N 37 *et seq.* <https://jusletter.weblaw.ch/juslissues/2017/891/the-position-of-bloc_6c88d13bf7.html> accessed 19 March 2023.

98 Bahar (n 97).

> This opportunity could also be used to fill the regulatory gap in regard to negotiable securities.
>
> While problems also arise with respect to the localisation of certain links such as the place of performance of a contract or the place of issue of equity securities or bonds, this is a general consequence of digitalisation that is not specific to blockchains. The answer to these questions should be left to the courts. This is even more important in light of the courts' ability to take European case law into account as well.
>
> In the area of court jurisdiction and the recognition of foreign judgments, many rules are already laid down by the Lugano Convention. Switzerland can exert only very limited influence on these rules.[99]

Based on the above observations, most rules of the PILA applicable to tokens are satisfactory. If the token is linked to a claim, the applicable law will be determined by art. 116 *et seq*. of the PILA;[100] if it is linked to a membership right, art. 154 para. 1 of the PILA will apply,[101] whereas prospectus liability actions fall under art. 156 of the PILA;[102] if it is linked to a right *in rem*, the governing law is determined by art. 99 *et seq*. of the PILA.[103] Those rules are still applicable after the PILA was modified by the DLT Act because the amendments do not relate to conflict-of-laws provisions regarding contracts, companies or rights *in rem*, but concern the transfer of claims by means of an instrument. We will not further examine the aforementioned rules as the Federal Council already proceeded to conduct a thorough, convincing analysis easily available online, to which we refer the reader.[104] Rather, the next section will focus in detail on the amended rules by the DLT Act, *i.e.* the rules regarding tokenised claims.

3 Amendments to the Swiss PILA

3.1 *Genesis*

The amendment of the PILA is part of a more general revision of different laws to create a favourable legal framework for the development of DLT

99 Federal Council report (n 1), 78.
100 *Id*., 74.
101 *Id*., 75.
102 *Id*., 76.
103 *Id*., 75 et seq.
104 *Id*., 70 et seq.

in Switzerland. In addition to the PILA, no less than nine federal laws were amended[105]: the Code of Obligations,[106] the Debt Enforcement and Bankruptcy Act,[107] the National Bank Act,[108] the Banking Act,[109] the Financial Services Act,[110] the Financial Institutions Act,[111] the Anti-Money Laundering Act,[112] the Intermediated Securities Act (FISA),[113] and the Financial Market Infrastructure Act.[114] The DLT Act is therefore structured as a framework act (*acte modificateur unique* or *Mantelerlass*) amending different laws rather than adopting a *lex specialis* applicable to DLTs.[115]

This section will outline which objectives were pursued by the legislator in amending those laws (3.1.1) and the legislative process that was followed until the DLT Act came into force (3.1.2).

3.1.1 General Objectives of the DLT Act

As a general rule, the DLT Act aims to further improve the framework conditions for DLT in Switzerland.[116] More specifically, the Dispatch of the Federal Council mentions three different objectives of the DLT Act: (i) increase legal certainty, (ii) remove obstacles to DLTs or blockchain-based applications, and

105 Message du Conseil Fédéral relatif à la loi fédérale sur l'adaptation du droit fédéral aux développements de la technologie des registres électroniques distribués, 27 November 2019, FF 2020 223, 249 *et seq.* («FF 2020»); Bahar (n 97), 18.

106 SR 220 (n 86).

107 Bundesgesetz über Schuldbetreibung und Konkurs (SchKG) vom 11. April 1889, AS 11 529, SR 281.1.

108 Federal Act on the Swiss National Bank (National Bank Act, NBA) of 3 October 2003, AS 2004 1985, SR 951.11.

109 Federal Act on Banks and Savings Banks (Banking Act, BA) of 8 November 1934, AS 51 117, SR 952.0.

110 Federal Act on Financial Services (Financial Services Act, FinSA) of 15 June 2018, AS 2019 4417, SR 950.1.

111 Federal Act on Financial Institutions (Financial Institutions Act, FinIA) of 15 June 2018, AS 2018 5247, SR 954.1.

112 Federal Act on Combating Money Laundering and Terrorist Financing (Anti-Money Laundering Act, AMLA) of 10 October 1997, AS 1998 982, SR 955.0.

113 Federal Act on Intermediated Securities (Federal Intermediated Securities Act, FISA) of 3 October 2008, AS 2009 3577, SR 957.1.

114 SR 958.1 (n 74).

115 See FF 2020 (n 105), 230; Federal Council report (n 1), 13; Hans Kuhn, "Digitale Aktiven im schweizerischen Privatrecht" in Rolf H. Weber and Hans Kuhn (eds), *Entwicklungen im Schweizer Blockchain-Recht* (Helbing Lichtenhahn 2021), 60, N 17.

116 Luca Bianchi, "An Introduction to the New Rules for Digital Assets" (2020) 1 CapLaw 2; Daniel Girsberger and Dirk Türten, "Entwicklungen im schweizerischen internationalen Privatrecht / Le point sur le droit international privé" (2021) Revue Suisse de Jurisprudence 224, 225.

(iii) limit new risks with respect to such technologies.[117] As DLT has significant potential for innovation and efficiency gains in different sectors of the economy, especially in the financial sector, these goals tend to provide a favourable legal framework to develop digitalisation of the economy through DLT.[118] With regard to such technologies, the Federal Council believes that "the best possible framework conditions must be created so that Switzerland can establish and further develop itself as a leading, innovative, and sustainable location for fintech and blockchain companies."[119] Moreover, this authority wants to ensure the "integrity and good reputation of Switzerland as a financial center and business location in this area as well. The risks associated with the spread of new technologies should therefore be addressed proactively, and abuses must be combated rigorously."[120]

To fulfil these objectives, especially to promote digitalisation as efficiently as possible, the legislator had to be careful not to hinder innovation and privilege some technologies instead of others. Accordingly, the DLT Act does not refer explicitly to a type of DLT or to another technology.[121] It is designed to be technology-neutral, which is a principle that is frequently followed by the Swiss legislator.[122] As a result, the DLT Act is not geared to any individual technology, but treats comparable activities and risks equally in principle wherever possible and reasonable.[123] According to the Federal Council, "especially in a rapidly changing technological environment, the development of which can be predicted only to a limited extent by lawmakers, this approach has proved itself. Firstly, it offers a high degree of flexibility. Secondly, it supports the objective of competitive neutrality. Thirdly, a technology-neutral approach alleviates the potential problem that sustainable legislative processes often lag behind technological progress. However, this should not rule out the possibility that there may be exceptional areas in which a specific legal adjustment is called for in

117 FF 2020 (n 105), 230.

118 Federal Council report (n 1), 11.

119 *Id.*

120 *Id.*

121 Hans Kuhn and Rolf H. Weber, "Einleitung" in Rolf H. Weber and Hans Kuhn (eds), *Entwicklungen im Schweizer Blockchain-Recht* (Helbing Lichtenhahn 2020), 6, N 20. See also in this sense Bahar (n 97), 18.

122 See Franca Contratto, "Technologie und Finanzmarktregulierung. Narrative von Interdependenz und Co-Evolution," in Rolf H. Weber et al. (eds), *Aktuelle Herausforderungen des Gesellschafts- und Finanzmarktrechts Festschrift für Hans Caspar von der Crone zum 60. Geburtstag* (Schulthess 2017), 435; Pascal Favrod-Coune and Vincent Pignon, *La Fintech en Suisse. Aspects réglementaires et économiques* (Schulthess 2021), 100.

123 Federal Council report (n 1), 13.

regard to distributed ledger or blockchain technology."[124] In addition, the rules must not tilt the competitive level playing field in order not to advantage one entity over another.[125]

As mentioned, the DLT Act amended a number of different acts, including the PILA. Swiss legal scholars have frequently outlined the difficulties that are caused by DLT in PIL,[126] as DLT is by nature not tied to a specific jurisdiction and the system of a blockchain itself is international.[127] As Guillaume explains, "the blockchain calls the traditional approach of private international law into question, since in reality it is impossible to establish the geographical location of blockchain transactions."[128] Such transactions sometimes concern many jurisdictions.[129] It is also occasionally excessively difficult, if not impossible, to determine the location of a token. Its applicable law can therefore be complicated to determine, and traditional conflict-of-laws rules are difficult to apply.[130] That being said, the DLT Act logically applies only if Swiss law is applicable to a transaction or to a token.[131] To meet the goals of the DLT Act, it was hence a necessity to examine to what extent Swiss PIL was suited to such technologies, and whether amendments were needed.

3.1.2 Legislative Process

In the last few years, both the private and the public sector worked on the steps necessary to include DLT into the Swiss legal order.[132]

---

124 *Id.*

125 *Id.*; FF 2020 (n 105), 229.

126 For example: Florence Guillaume, "Aspects of Private International Law Related to Blockchain Transactions," in Daniel Kraus, Thierry Obrist, and Olivier Hari (eds), *Smart Contracts, Decentralised Autonomous Organizations and the Law* (Elgar 2019), 60 et seq.; Florence Guillaume, "Blockchain. Le pont du droit international privé entre l'espace numérique et l'espace physique," in Ilaria Pretelli (ed), *Le droit international privé dans le labyrinthe des plateformes digitales* (Schulthess 2018), 174 *et seq.* With regard to bitcoins, see Graham-Siegenthaler and Furrer (n 97), N 20 et seq.

127 Guillaume, "Blockchain" (n 126), 175; Joël Leibenson and Frédéric Bétrisey, "La mise en gage d'actions représentées par des jetons numériques (tokens)," in Rita Trigo Trindade, Rashid Bahar, and Giulia Neri-Castracane (eds), *Vers les sommets du droit - Liber amicorum pour Henry Peter* (Schulthess 2019), 70.

128 Guillaume, "Aspects" (n 126), 70. See also Graham-Siegenthaler and Furrer (n 97), N 34.

129 Kuhn (n 115), 117, N 198.

130 *Id.*

131 A reserve must however be made with regard to the *lois d'application immédiate* pursuant to art. 18 or 19 of the PILA (n 2), such as some rules regulating financial markets, see for example Favrod-Coune (n 30), N 1199 and the cited references.

132 Kuhn and Weber (n 121), 4, N 11.

At the private sector level, the efforts of the Swiss Blockchain Federation are particularly noteworthy. This Federation established a taskforce, which in April 2018 published a White paper entitled "Strengthening the blockchain in Switzerland," in which several needed improvements to the existing legal framework were identified.[133]

From a political viewpoint, different initiatives[134] were undertaken by the members of the Parliament: three motions,[135] five interpellations[136] as well as two postulates.[137] In addition, the Federal Council published in December 2018 a report on the legal framework for DLT and blockchain in Switzerland, prepared by members of different federal authorities, including the FINMA and the Swiss National Bank.[138] In drafting this report, the recommendations of the Swiss Blockchain Federation mentioned above were considered and numerous discussions with representatives from the industry working in the financial sector, law firms and business associations were held.[139]

The 162-pages report published in December 2018 examines extensively how the Swiss legal framework applies to DLT from a perspective of civil and insolvency law, as well as from a financial markets law viewpoint, including

133 The White paper is available at Blockchain Taskforce, "Strengthening the blockchain in Switzerland: The White Paper of the Blockchain Taskforce" (*Blockchain Federation*, April 2018) <https://blockchainfederation.ch/wp-content/uploads/2018/10/Blockchain-Taskforce-White-Paper_English-Version1.pdf> accessed 19 March 2023. See also Federal Council report (n 1), 14; Kuhn and Weber (n 121), 4, N 11.

134 See Federal Council report (n 1), 12; Kuhn and Weber (n 121), 4, N 11, footnote 14.

135 Claude Béglé, Motion 17.3818 "Die Schweiz zu einem Weltzentrum der Blockchain-Technologie machen" (28 September 2017); Claude Béglé, Motion 16.3484 "Conforter la position dominante de la Suisse dans la technologie 'blockchain'" (16 June 2016), and Giovanni Merlini, Motion 17.4035 "Blockchain-Anwendungen und Kryptowährungen. Es braucht eine Anpassung der verfahrensrechtlichen Instrumente der Justiz- und der Verwaltungsbehörden" (7 December 2017).

136 Guillaume Barazzone, Motion 18.3272 "Kryptofranken für die Schweiz?" (15 March 2018); Leo Mueller, Motion 17.4144 "Kryptowährungen. Besteht Handlungsbedarf?" (14 December 2017); Ruedi Noser, Motion 17.4213 "Attraktivität der Schweiz als Standort für Fintech-Unternehmen" (14 December 2017); Martin Schmid, Motion 17.4024 "Risques et opportunités inhérents aux bitcoins et aux cybermonnaies" (6 December 2017), and Elisabeth Schneider-Schneiter, Motion 16.3272 "La Svizzera e la sfida della tecnofinanza" (26 May 2016).

137 Cédric Wermuth, Motion 18.3159 "Bericht zu Möglichkeiten, Chancen und Risiken der Einführung eines Kryptofrankens" (14 March 2018) and Commission for Economic Affairs and Taxation Committee of the National Council, Postulate 15.4086 "Für einen wettbewerbsfähigen Finanzplatz im Bereich neuer Finanztechnologien" (10 November 2015).

138 Federal Council report (n 1), 14; Kuhn and Weber (n 121), 4, N 11.

139 Federal Council report (n 1), 14.

anti-money laundering aspects.[140] This report does not only explain how to apply Swiss law to DLT applications, but also identifies several courses of action and proposes concrete amendments to better conciliate the Swiss legal framework and add clarity in this respect.

This report built the foundations to the adoption of the DLT Act. Approximately four months later, the Federal Council published a preliminary draft bill (*avant-projet* or *Vorentwurf*) of the DLT Act on 22 March 2019.[141] Thereafter, a consultation period began, during which all stakeholders and authorities could share their view and provide commentaries on the proposed bill. A report on the results of the consultation process was published on 27 November 2019.[142] On the same day, a draft bill (*projet* or *Entwurf*) was issued, together with a Dispatch explaining the envisaged provisions.[143]

The draft bill was examined by both the National Council and States Council during the summer session 2020. On 25 September 2020, it was unanimously approved with 196 votes to 0,[144] respectively 44 to 0.[145]

Shortly after the positive vote of the Parliament, the Federal Department of Finance published a draft DLT Ordinance on 19 October 2020.[146] This Ordinance is designed to incorporate the legislative amendments voted for by the Parliament in the field of insolvency and financial markets law. The other provisions, especially in civil law and PIL, amended by the DLT Act did not have to be implemented and completed in a federal Ordinance. As a result, those provisions could be put into force immediately. The Federal Council announced on 11 December 2020 that the amendments to the CO, the Intermediated Securities Act and the PILA would enter into force on 1 February 2021,

140 *Id.*

141 Swiss Federal Council, "Federal Council opens consultation on improving the legal framework governing blockchain and TRD" (*Federal Council*, 22 March 2019) <https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-74420.html> accessed 19 March 2023.

142 Swiss Department of Finance (DFF), "Consultation relative à la loi fédérale sur l'adaptation du droit fédéral aux développements de la technologie des registres électroniques distribués – Rapport sur les résultats" (*DFF*, 27 November 2019) <https://www.newsd.admin.ch/newsd/message/attachments/59308.pdf> accessed 19 March 2023. This report was especially brief considering the amendments of the PILA, only stating that the few opinions expressed on the amendments to the PILA were positive. At most, they contained a few proposals for clarification. See *id.*, 11.

143 FF 2020 (n 105), 224 et seq.

144 Bulletin officiel du Conseil National (BOCN) 2020, 1959.

145 Bulletin officiel du Conseil des États (BOCE) 2020, 1073.

146 DFF, "Lancement de la consultation concernant l'acte modificateur unique dans le domaine de la blockchain" (*DFF*, 19 October 2020) <https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-80775.html> accessed 19 March 2023.

while all other provisions needed to wait until the definitive version of the DLT Ordinance is adopted.[147] Those entered into force on 1 August 2021.[148] Overall, approximately three years passed from the publication of the first report in December 2018 to the entry into force of the DLT Act, which is a relatively short timeframe for the adoption of a law in Switzerland.[149]

3.2 *New Provisions of the PILA with Regard to Tokens*

The DLT Act did not create a new *sui generis* category in the PILA for tokens.[150] However, adjustments to the existing PILA were made in order to provide legal certainty for transactions based on a DLT.[151] To accomplish this, four different provisions of the PILA were amended by the DLT Act. The new provisions or versions entered into force on 1 February 2021.

Firstly, a new art. 145a of the PILA was introduced, which sets forth the following:

1. "Whether a claim is represented by an instrument in paper or equivalent form and transferred by means of such instrument is determined by the law designated therein. If no law is designated in the instrument, the law of the state in which the issuer has its seat or, failing such, its habitual residence applies."
2. "As regards rights in rem to a physical instrument, the provisions of Chapter 7 [i.e. art. 97 to 108 of the PILA] are reserved."

Secondly, art. 106 of the PILA was modified as follows:

1. "The law designated in Article 145a paragraph 1 determines whether an instrument represents goods."
2. "If the goods are represented by a physical instrument, the rights in rem to both the instrument and the goods are governed by the law applicable to the instrument as movable property"
3. "If several persons assert rights in rem relating to the goods, some directly, others on the basis of an instrument, the law applicable to the goods themselves determines which one of these rights prevails."

---

147 Swiss Federal Council, "Federal Council brings part of DLT bill into force" (*Federal Council*, 11 December 2020) <https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-81563.html> accessed 19 March 2023. See also Kuhn and Weber (n 121), 5, N 15.

148 Swiss Federal Council, "Le Conseil fédéral met en vigueur le reste de la loi sur la TRD et édicte l'ordonnance qui s'y rapporte" (*Federal Council*, 18 June 2021) <https://www.admin.ch/gov/fr/accueil/documentation/communiques/communiques-conseil-federal.msg-id-84035.html> accessed 19 March 2023.

149 Same opinion, Kuhn and Weber (n 121), 5, N 16.

150 Bahar (n 97), 18.

151 *Id.*

The new art. 145a of the PILA and the amendment of art. 106 of the PILA are the main rules used to determine the applicable law to tokens (*infra* 3.2.1).

Thirdly, the wording of art. 105 para. 2 of the PILA was amended:

"In the absence of a choice of law, the pledging of claims is governed by the law of the state of the pledgee's habitual residence. The same applies to the pledging of other rights, provided they are represented by an uncertificated security, a certificated security or an equivalent instrument; otherwise, the pledging of such rights is governed by the law applicable to them."

This amendment is an exception to the general rules expressed in art. 145a and 106 of the PILA (*infra* 3.2.2).

Finally, art. 108a of the PILA has also been amended and is now formulated as follows:

"Intermediated securities are securities held with an intermediary as defined in the Hague Convention of July 5, 2006 on the Law Applicable to Certain Rights in Respect of Securities held with an Intermediary."

This amendment, however, only applies to the German version of the PILA, but not to the French and Italian ones, since the aim of the amendment is to clarify the meaning of art. 108a of the PILA in the German language version.[152] The notion of securities is to be interpretated in the sense of the Hague Convention of 5 July 2006 on the Law Applicable to Certain Rights in Respect of Securities held with an Intermediary,[153] which is wider than the one used by art. 105, 106 and 145a of the PILA.[154] The previous German version of art. 108a of the PILA was ambiguous and potentially misleading, so it was necessary to formally clarify its scope of application. Its new wording also avoids referring to the custody of the securities through "*einem Intermediär*," which were considered deceptive by commentators,[155] and rightly prefers the specific term "*intermediärverwahrtes Wertpapier*" also used by the Hague Convention. With the adoption of art. 145a of the PILA, this amendment is in our opinion to be welcomed because it avoids any misconception and issues of interpretation of art. 108a of the PILA.

152 FF 2020 (n 105), 287.

153 Convention on the Law Applicable to Certain Rights in Respect of Securities held with an Intermediary, AS 2017 2081, SR 0.221.556.1.

154 FF 2020 (n 105), 287; Florence Guillaume, "art. 108a," in Andreas Bucher (ed), *Commentaire romand. Loi fédérale sur le droit international privé* (LDIP)/ *Convention de Lugano* (CL) (Helbing Lichtenhahn 2011), N 2.

155 Hans Kuhn, "Art. 108a," in Markus Müller-Chen and Corinne Widmer Lüchinger (eds), *Zürcher Kommentar zum IPRG. Kommentar zum Bundesgesetz über das Internationale Privatrecht* (IPRG) *vom 18. Dezember 1987* (*2 Bände*) (Schulthess 2018), N 2.

3.2.1 General Principle to Determine the Law Applicable to Tokens

As we have explained, a token is not more than a piece of information that gives a person, *i.e.* the person owning the private key related to the token, the right embedded in said token.[156] The PILA, as amended by the DLT Act, assumes that the right embedded in a token is neither a proper claim (*créance* or *Forderung*) nor a negotiable instrument (*papier-valeur* or *Wertpapier*), but a special form of intangible instrument (*droit-valeur* or *Wertrecht*).[157] As a result, the PILA cannot treat a token as one of those legal entities and specific conflict-of-laws rules cannot apply. In particular, art. 145 of the PILA sets forth that the assignment of a claim by contract is governed by the law chosen by the parties or, in the absence of such choice, by the law applicable to the assigned claim. It is therefore applicable to an assignment of a claim by contract,[158] but if the claim is represented by a document, art. 145 of the PILA is not applicable.[159] Accordingly, the assignment of a claim incorporated in a token does not fall under this provision.[160] However, in the eyes of the Federal Council, it must be treated as a claim embedded in a negotiable instrument.[161] In order to provide a specific legal framework for this special form of book-entry instrument, including in particular for tokens, the legislator adopted art. 145a of the PILA.[162]

The wording of art. 145a para. 1 of the PILA determines its scope of application. Firstly, it applies to claims that are represented "by an instrument in paper or equivalent form." *Inter alia,* it could apply to claims embedded in:

- book-entry securities pursuant to art. 973c of the CO,[163] which can replace fungible negotiable securities or global certificates that have been entrusted to a single custodian with book-entry securities.
- ledger-based securities pursuant to art. 973d of the CO:[164] such instrument is a right which, in accordance with an agreement between the parties, (i) is registered in a securities ledger following several requirements set forth by

156 See *supra* sec. 2.1.

157 Bahar (n 97), 18. See also Federal Council report (n 1), 76.

158 Andreas Bonomi, "art. 145," in Andreas Bucher (ed), *Commentaire romand. Loi fédérale sur le droit international privé* (LDIP)/*Convention de Lugano* (CL) (Basel: Helbing Lichtenhahn 2011), N 3.

159 *Id.*, N 5.

160 Federal Council report (n 1), 76.

161 *Id.*

162 Bahar (n 97), 18.

163 FF 2020 (n 105), 287 et seq. that refers to "équivalent (immatériel) d'un papier-valeur"; Bahar (n 97), 19.

164 FF 2020 (n 105), 288; Deborah De Col, *Zivilrechtliche Herausforderungen der Blockchain-Technologie*, Thomas Sutter-Somm (ed) (Zurich, Basel and Geneva: Schulthess 2021), N 160.

art. 973d para. 2 of the CO, and (ii) may be exercised and transferred to others only via this securities ledger. This provision has also been adopted with the DLT Act and entered into force simultaneously with art. 145a of the PILA. Many types of tokens can be issued as ledger-based securities, provided they embed a claim against the issuer.[165] Tokens representing shares, bonds or other financial instruments can therefore be issued as ledger-based securities under Swiss law.[166] However, pure cryptocurrencies cannot be issued as such instruments because they constitute a means of payment based on the principles of cryptography and are not issued by a central issuer against which a claim can be exercised.[167]

– Other instruments in equivalent form:[168] since the wording of art. 145a para. 1 of the PILA is very wide, other instruments that are not conceived as securities pursuant to the CO are also covered by this provision, provided that they can be used as a negotiable instrument.[169] The medium in which the claim is incorporated can be either tangible or intangible.[170] The crucial element is that the claim must be linked in some way to a text from which the content of the claim is apparent, and it must be possible to link the claim to a holder who must in its turn be able to transmit it to another person.[171] While being drafted in wide terms, art. 145a para. 1 of the PILA does not mention any specific technology, in accordance with the principle of technological neutrality. This allows the provision to apply not only to several types of tokens independently on which blockchain they are issued, but also to others electronic instruments, such as e-mails or their attachments.[172]

Secondly, art. 145a para. 1 of the PILA makes clear that the claim must be transferred "by means of such instrument," *i.e.* an instrument as described above. Of course, this notion refers primarily to the transfer of the claim through

165 Favrod-Coune and Pignon (n 122), 156; Stefan Kramer and Urs Meier, "Tokenisierung von Finanzinstrumenten. Gemäss dem Entwurf des Bundesgesetzes zur Verbesserung der Rahmenbedingungen für Blockchain/DLT" (2020) 1 Gesellschafts- und Kapitalmarktrecht 60, 65.

166 FF 2020 (n 105), 266 *et seq.*; Favrod-Coune and Pignon (n 122), 156; Stefan Kramer, David Oser, and Urs Meier, "Tokenisierung von Finanzinstrumenten de lege ferenda. Unter besonderer Berücksichtigung von nicht kotierten Aktien" (*Jusletter*, 6 May 2019), N 22 <https://jusletter.weblaw.ch/juslissues/2019/978/tokenisierung-von-fi_cac04a76c5.html> accessed 19 March 2023.

167 FF 2020 (n 105), 267; Favrod-Coune and Pignon (n 122), 156; Houdrouge and Tenot (n 62), 60.

168 FF 2020 (n 105), 288; Bahar (n 97), 19.

169 FF 2020 (n 105), 288.

170 *Id.*

171 *Id.*; De Col (n 164).

172 FF 2020 (n 105), 288; Bahar (n 97), 19.

the instrument.[173] This is traditionally how a claim embedded in a negotiable instrument is assigned to another person. However, this way of assignment is often not available for the transfer of tokens. Rather than being properly transferred, tokens are replaced by a new token embedding a similar claim, which is owned by the acquirer of the token. Accordingly, even though the wording of art. 145a para. 1 of the PILA does not explicitly consider this hypothesis, such means of transfer also fall under the scope of this provision, as confirmed by the Dispatch of the Federal Council.[174] Art. 145a para. 1 of the PILA therefore applies to different types of transactions involving the title that transfer the claim.

Nevertheless, art. 145a para. 1 of the PILA is not applicable to all types of instruments. Firstly, its scope of application does not extend to book-entry securities that are registered in a centrally-kept register and that can be only transferred by an entry in such register.[175] For such instruments, the place where the register is kept, *i.e.* the *lex libri sitae*, should preferably be applicable as the transfer necessarily occurs at the place of the register. Kuhn convincingly argues that in such circumstances, the scope of art. 145a para. 1 of the PILA should be limited according to the purpose of the provision ("*teleologisch zu reduzieren*").[176] Secondly, this provision is equally not applicable to intermediated securities[177] because art. 108a *et seq*. of the PILA, which refers to the Hague Convention of 5 July 2006 on the Law Applicable to Certain Rights in Respect of Securities held with an Intermediary, are *lex specialis* to art. 145a para. 1 of the PILA.[178] The law applicable to the transfer of such instruments is determined by art. 108c of the PILA and the Hague Convention of 5 July 2006 on the Law Applicable to Certain Rights in Respect of Securities held with an Intermediary.[179]

It is unclear whether art. 145a para. 1 of the PILA applies to negotiable instruments physically embedded in a paper (*papiers-valeurs* or *Wertpapiers*). Both the wording of art. 145a of the PILA and the Dispatch of the Federal Council are

173 FF 2020 (n 105), 288.

174 *Id.*

175 Kuhn (n 115), 125, N 220.

176 *Id.*

177 In this context, intermediated securities refer to securities according to art. 3 PISA that are held by custodians pursuant to art. 4 PISA. For more detail on the notion of intermediated securities, see Luc Thévenoz and Antoine Eigenmann, "Intro LTI," in Tercier Pierre, Amstutz Marc, and Trigo Trindade Rita (eds), *Commentaire romand. Code des obligations II* (Helbing Lichtenhahn 2017), N 71 *et seq.*, 144 *et seq.*

178 Kuhn (n 115), 125, N 220.

179 FF 2020 (n 105), 289.

somewhat confusing in this respect.[180] Art. 145a para. 1 of the PILA states that it applies to instruments in paper form, whereas art. 145a para. 2 of the PILA sets forth that rights *in rem* concerning a physical instrument are governed by art. 97 to 108 of the PILA. Moreover, the Dispatch explains that art. 145a of the PILA indicates the law to be applied in determining if a claim is represented by an instrument, whether it is in the form of paper or an equivalent form, in other terms whether it is a negotiable instrument physically embedded in a paper or the (immaterial) equivalent.[181] At the same time, the Dispatch also explains that if the law applicable under art. 145a para. 1 of the PILA establishes a link between the transfer of the claim and the transfer of ownership of the instrument, the aspects relating to rights *in rem* are regulated in accordance with art. 145a para. 2 of the PILA, which means that aspects relating to rights *in rem* are governed by the provisions of Chapter 7 of the PILA. As a result, the law of the place where the negotiable instrument is located (*lex chartae sitae*) determines whether ownership of the negotiable instrument has been transferred.[182] Moreover, the Dispatch states that art. 145a para. 2 of the PILA only apply to physical titles, hence the specification of physical instrument in the wording.[183] Kuhn argues that the transfer of directly held physical instruments is also covered by the scope of application of art. 145a para. 2 of the PILA, so that art. 145a para. 1 of the PILA resultantly only applies to the transfer of non-physical instruments.[184] According to this author, it appears from the preparatory works of the DLT Act that the legislator did not contemplate any amendment with regard to negotiable instruments, but only wanted the law to apply to tokenised claims.[185] In our opinion, this argument seems to be in direct contradiction with the wording of art. 145a para. 1 of the PILA, which

180 Same opinion, Kuhn (n 115), 123–24, N 215.

181 FF 2020 (n 105), 289: "L'art. 145a P-LDIP indique le droit qu'il convient d'appliquer pour déterminer si une créance est représentée par un titre, qu'il revête la forme d'un papier ou une forme équivalente, soit, en d'autres termes, si l'on se trouve en présence d'un papier-valeur ou de l'équivalent (immatériel) d'un papier-valeur."

182 *Id.*: "Si le droit applicable selon l'art. 145a, al. 1, P-LDIP établit un lien entre le transfert de la créance et le transfert de la propriété du titre, les aspects relatifs aux droits réels seront réglés, conformément à l'al. 2, selon les dispositions du chapitre 7 de la loi («Droits réels»). Le droit du lieu de situation du titre (lex chartae sitae) déterminera si la propriété de ce dernier a été transférée."

183 *Id.*: "L'art. 145a, al. 2, P-LDIP ne s'appliquera qu'aux titres matériels, d'où la précision «titre physique»."

184 Kuhn (n 115), 125, N 219: "Die Übertragung von direkt gehaltenen physischen Wertpapieren ist deshalb ebenfalls vom Vorbehalt in Art. 145a Abs. 2 IPRG erfasst, sodass Art. 145a Abs. 1 IPRG im Ergebnis nur für die Übertragung von nicht-physischen Titeln gilt."

185 *Id.*

explicitly mentions negotiable instruments issued on paper. Moreover, the Report of December 2018 explains that "[l]egislative clarification in the form of a supplementary provision in the PILA [*i.e.* the new art. 145a of the PILA] appears called for in this regard. This opportunity could also be used to fill the regulatory gap regarding negotiable securities."[186] It seems to us that the legislator wanted to include negotiable instruments in art. 145a para. 1 of the PILA, as the provision's wording suggests. In any case, such analysis should not be of practical relevance for tokens stored on a DLT, as they should not constitute physical instruments, so that art. 145a para. 1 of the PILA should apply to them.

When art. 145a para. 1 of the PILA applies, it sets forth a conflict-of-laws rule that is divided into a principal and a subsidiary rule.

The principal rule is that the law designated in the instrument determines whether the instrument represents a right and whether the right is transferred through the instrument (first sentence).[187] The chosen law by the parties is therefore decisive and art. 145a para. 1 of the PILA provides for no restriction in this regard. The choice does not have to be in a specific form and the chosen law does not need to have a minimal connection with the instrument.[188] Moreover, there is no limitation regarding the participation of a consumer, unlike that for consumer contracts pursuant to art. 120 of the PILA. In practice, a protective provision such as art. 120 of the PILA would most likely not have been useful as the issuance of instruments covered by art. 145a para. 1 of the PILA usually does not target consumers,[189] *i.e.* persons who acquire goods or services for ordinary consumption intended for their personal or family use and not connected with their professional or business activity.[190] It is noteworthy that, unlike a choice of law for a contract (art. 116 para. 3 of the PILA) or for rights *in rem* (art. 104 para. 2 of the PILA), this choice of law is applicable *erga omnes* and is not limited to the parties.[191] It can therefore be applicable to third parties. For tokens issued on a DLT, this solution is based on the fact that

186 Federal Council report (n 1), 78.

187 Bahar (n 97), 19; De Col (n 164), N 159.

188 Kuhn (n 115), 126, N 221.

189 *Id.* We note that the Hague Convention of 5 July 2006 on the Law Applicable to Certain Rights in Respect of Securities held with an Intermediary also does not provide for a limitation for consumer; see *id.*; Martin Peyer, "Probleme der Rechtswahl nach Haager Wertpapier-Übereinkommen im Depotvertrag" (2007) 17 Aktuelle Juristische Praxis 956, 966.

190 See Andrea Bonomi, "art. 120," in Andreas Bucher (ed), *Commentaire romand. Loi fédérale sur le droit international privé* (LDIP)/ *Convention de Lugano* (CL) (Helbing Lichtenhahn 2011), N 9.

191 Kuhn (n 115), 126, N 222.

third parties can only acquire rights embedded in a token if they participate in the DLT system and accept the participating conditions, which is deemed as a consent to a choice of law clause.[192]

The subsidiary rule applies if the instrument does not provide for an applicable law. Absent a choice of law, the law of the seat of the issuer or, failing such, of its habitual residence applies (second sentence).[193] In this context, the issuer is the person that becomes the debtor of the claim and not the technical issuer of the token, unless both are the same.[194] The seat of the issuer is determined by art. 21 para. 2 of the PILA, which refers to the place designated in the articles of incorporation or in the articles of association or, in the absence of such designation, where the company is administered in fact. The habitual residence is to be interpreted in accordance with art. 20 para. 1 lit. b of the PILA; this provision refers to the place at which a person lives for a certain period of time, even if this period is of limited duration from the outset.

As Bahar explains, the solutions provided by this conflict-of-laws rule are "not revolutionary, nor even new"[195] because they were already applicable to specific types of instruments. The Dispatch of the Federal Council explicitly mentions that art. 145a para. 1 of the PILA is inspired by art. 106 of the PILA, which applies to titles to goods (*titres représentatifs de marchandises* or *Warenpapiere*), and was, until 1 February 2021, the only conflict-of-laws rule of the PILA to address the transfer of securities, outside intermediated securities.[196] The principles established for titles to goods were taken as a guideline to adopt art. 145a of the PILA, however with a few differences.[197] As we have seen above,[198] art. 106 of the PILA was also amended by the DLT Act. This is because art. 1153a of the CO adopted with the DLT Act explicitly allows the titles to goods to be issued digitally in the form of ledger-based securities pursuant to art. 973d *et seq*. of the CO.[199] The conflict-of-laws rule of art. 106 of the PILA therefore had to be amended accordingly in order to be consistent with the new legal framework providing for titles to goods. Hence, art. 106 para. 1 of the PILA refers to the solution now provided by art. 145a para. 1 of the PILA to determine whether there is a title to goods and to what extent this title entails a right of ownership to the goods, in addition to the existence of a right to have them

192 *Id.*
193 Bahar (n 97), 19; De Col (n 164), 126, N 223.
194 Kuhn (n 115), 126, N 223.
195 Bahar (n 97), 19.
196 FF 2020 (n 105), 288.
197 See *infra* sec. 3.3.1.
198 See *supra* sec. 3.2.
199 See FF 2020 (n 105), 280; Kuhn (n 115), 85, N 88.

delivered.[200] The reason behind the repeal of the former conflict-of-laws rule of art. 106 para. 1 of the PILA and its replacement by this reference is that the right to have the goods delivered is also a claim embedded in an instrument within the meaning of art. 145a para. 1 of the PILA.[201] The German wording of art. 106 para. 1 and 3 of the PILA that mentioned "*Papier*" also needed to be replaced by "*Title*" in order to include intangible instruments.[202] As a result, defining whether a title represents goods is determined by the law indicated by the title and, failing one, by the law of the seat of the issuer or its habitual residence.[203] This rule will, in principle, apply to asset tokens that aim to embed a right *in rem* on movable assets.[204] However, despite the amendment, it is not possible to incorporate rights to real estate through DLTs from a conflict-of-laws perspective, as art. 99 para. 1 of the PILA will continue to apply in this regard.[205]

As briefly mentioned above, art. 145a para. 2 of the PILA reserves the application of art. 97 to 108 of the PILA with regard to rights *in rem* concerning physical instruments. In such a case, the law of the place where the instrument is located, *i.e.* the *lex chartae sitae*, applies.[206] For tokens based on a DLT, this rule will not apply in practice since a right recorded on a distributed ledger cannot be tied to a specific physical location.[207] Consequently, the rules provided by art. 145a para. 1 of the PILA will determine the applicable law for tokens issued on a DLT.

3.2.2 Exception for the Pledging

The principles expounded above do not apply to the pledging (*mise en gage* or *Verpfändung*) of instruments and claims mentioned by art. 145a para. 1 of the PILA. The art. 105 of the PILA is indeed a *lex specialis* to determine the applicable law to pledging.[208] If art. 105 para. 1 of the PILA allows the parties to choose the applicable law just like art. 145a para. 1 first sentence of the PILA (with the

200 FF 2020 (n 105), 286 et seq.
201 *Id.*, 287.
202 *Id.*; Kuhn (n 115), 129, N 231. We note that art. 106 para. 2 of the PILA (n 2) did not need to be amended in such a way because this provision applies to rights *in rem* that cannot be immaterial. For the sake of clarity and uniformity, the noun "title" was however replaced by "physical title."
203 Bahar (n 97), 19.
204 *Id.*
205 *Id.*
206 *Id.*; FF 2020 (n 105), 289.
207 Bahar (n 97), 19.
208 Kuhn (n 115), 128–29, N 230.

notable exception that it does not apply *erga omnes*),[209] the subsidiary rule of art. 105 para. 2 of the PILA provides a different conflict-of-laws rule than art. 145a para. 1 second sentence of the PILA.[210]

The DLT Act amended art. 105 para. 2 of the PILA in order to clearly establish that the intangible equivalents to negotiable instruments are treated in the same way as proper negotiable instruments.[211] Accordingly, these provisions now set forth that the pledging of claims is governed by the law of the state of the pledgee's habitual residence. The same applies to the pledging of other rights, provided they are represented by an intangible instrument, a negotiable instrument or an equivalent instrument.[212] Unlike the solution established by art. 145a para. 1 of the PILA, it is not the law of the seat nor, absent one, the habitual residence of the issuer of the instrument that is pertinent to determine the applicable law, but the habitual residence of the secured creditor.[213]

3.3 *Critical Appraisal*

The Swiss PIL framework presented above is applicable as of 1 February 2021. This section will examine to which extent it is suited to practice, and discuss the choices made by the legislator.

As a preliminary point, we welcome the fact that the legislator did not decide to restrict the application of the amendments of the PILA to specific types of tokens or technologies. We have seen above that a fair number of new types of tokens are created on a regular basis.[214] Limiting the scope of application to the actual state-of-the-art with regards to tokenisation would have been a mistake because the PILA would have probably been outdated in the near future. The new law could not have been applied to new tokens, which would in our opinion have fallen into a new legal gap (*lacune de la loi* or *Gesetzeslücke*). The approach of the legislator not to adopt provisions that are restricted to a specific technology and to formulate the wording in a neutral technological manner allows for security of the future and to not compromise the aim of the DLT Act.

---

209 *Id.*; Leibenson and Bétrisey (n 127), 71. See also Louis Gaillard, "art. 105," in Andreas Bucher (ed), *Commentaire romand. Loi fédérale sur le droit international privé* (LDIP)/ *Convention de Lugano* (CL) (Helbing Lichtenhahn 2011), N 3.

210 Bahar (n 97), 20.

211 FF 2020 (n 105), 286.

212 If the right is not represented by such instrument, art. 105 para. 2 *in fine* of the PILA provides that the pledging of such rights is governed by the law applicable to them.

213 Bahar (n 97), 20; Kuhn (n 115), 128–29, N 230.

214 See *supra* sec. 2.1.

Some elements must however be discussed. We will first expose why the solution for instruments pursuant to art. 145a of the PILA is different than the one in former art. 106 para. 1 of the PILA (3.3.1), then present the consequences of not having adopted the same solution for the pledging of instruments as for the assignment of claims (3.3.2), and finally outline the consequences of not having adopted a proper provision for pure cryptocurrencies (3.3.3).

3.3.1 A Different Solution for Instruments Pursuant to Art. 145a of the PILA than for Titles to Goods Pursuant to Former Art. 106 Para. 1 of the PILA

As stated above, in order to elaborate art. 145a of the PILA, the legislator took inspiration from the solutions provided by art. 106 para. 1 of the PILA.[215] However, its solutions were not taken as such or applied by analogy in the context of art. 145a of the PILA. It is appropriate to reflect on the reasoning and the validity of this choice.

The report of the Federal Council suggested to apply the principles of former art. 106 of the PILA by analogy to tokens. It states the following: "the law chosen by the parties of the underlying contract is decisive or, where no such choice has been made, the law at the seat of the branch of the issuer. While [former] Article 106 para. 1 of the PILA requires that the chosen law be 'designated in the token,'" this requirement is likely to be met in most cases. The issuer designates the law in the token terms and conditions defined by the issuer. To what extent the law referred to in [former] Article 106 para. 1 of the PILA differs from the law applicable to the primary contract thus depends essentially on how the term 'branch' used in Article 106 para. 1 of the PILA should be interpreted."[216]

Before being amended by the DLT Act, former art. 106 para. 1 of the PILA used the notion of branch or establishment (*établissement* or *Niederlassung*) of the issuer as a subsidiary criterion to determine the applicable law. This notion refers to art. 20 lit. c of the PILA for natural persons and to art. 21 para. 3 of the PILA for companies.[217] For a natural person, an establishment is where the centre of his/her professional or commercial activities is located, whereas for a company it is where its seat is located or in any state where one of its

215 See *supra* sec. 3.2.1.

216 Federal Council report (n 1), 75.

217 Pius Fisch and Alexander Fisch, "Art. 106," in Pascal Grolimund, Leander D. Loacker, and Anton K. Schnyder (eds), *Basler Kommentar Internationales Privatrecht* (Helbing Lichtenhahn 2020), N 6; Markus Müller-Chen, "Art. 106," in Markus Müller-Chen and Corinne Widmer Lüchinger (eds), *Zürcher Kommentar zum IPRG. Kommentar zum Bundesgesetz über das Internationale Privatrecht (IPRG) vom 18. Dezember 1987 (2 Bände)* (Schulthess 2018), N 6.

branches is located. Based on these definitions, it is possible to have more than one establishment,[218] which makes the criterion of establishment somewhat less predictable than the domicile of a natural person or the seat of a company, which are both unique. This issue can lead to the risk of forum shopping or even forum running.

The imprecise nature of the notion of establishment used by former art. 106 para. 1 of the PILA is the reason why the legislator did not decide to follow the solutions provided by this provision and transpose them into art. 145a para. 1 of the PILA, which would have resulted in a modification of the legal framework applicable to titles to goods.[219] Rather, the seat of the company issuing the tokens was chosen as the most relevant criterion, as it is most easily identifiable for third parties.[220] The establishment was also not chosen even in the absence of a seat (for example if a natural person issues tokens), but the criterion of habitual residence was preferred. Would it have been preferable to have chosen the domicile, which is the equivalent of the seat for natural persons (art. 21 para. 1 of the PILA)? In our opinion, the domicile could have been a possibility, but the solution of the habitual residence is more suitable as it provides uniformity between the applicable law to a contract related to a token and the applicable law to the transfer of such instrument. The Dispatch seems to suggest this because art. 117 para. 2 of the PILA also provides for the habitual residence rather than the domicile.[221]

3.3.2 Legal Uncertainty for Pledging

Fundamentally, the principles that were applicable to pledging under art. 105 of the PILA by the DLT Act have not been changed by the amendment. Firstly, this provision still grants significant autonomy to the parties to choose the applicable law and does not limit the choice of the law, even though it does not apply *erga omnes*.[222] Secondly, absent a choice of law, it is the law of the habitual residence of the secured creditor that is applicable.

Theoretically, other criteria than the habitual residence of the secured creditor could have been chosen by the legislator: (i) the habitual residence of the

218 Florence Guillaume, "art. 21," in Andreas Bucher (ed), *Commentaire romand. Loi fédérale sur le droit international privé* (*LDIP*)/ *Convention de Lugano* (*CL*) (Helbing Lichtenhahn 2011), N 11; Edgar Philippin, "Migration et droit privé: influences réciproques, théorie des personnes physiques et morales, impact sur les rapports d'obligation et leur mise en œuvre" (2017) 136 Revue de droit suisse 313, 351 *et seq.*

219 FF 2020 (n 105), 289.

220 *Id.*; De Col (n 164), N 159.

221 FF 2020 (n 105), 289.

222 Gaillard (n 209).

debtor in the pledge, (ii) the law that applies to the pledged claim, or (iii) the place where the negotiable instrument is located, for such instrument.[223] The criterion of the habitual residence of the secured creditor was selected because the legislator has considered that the unity of the regime of the pledge transaction was better ensured if the applicable law is determined by the residence of the secured creditor.[224] Indeed, the law applicable to the claim or to the pledged instrument may be insecure since, in a pledge transaction, the claims or securities pledged may be diverse and subject to different laws.[225] As a result, the same pledge transaction could have been subject to different laws depending on the law applicable to each of the pledged assets.[226] In addition, negotiable instruments may be moved or deposited in foreign places, so that the place where they are located may be irrelevant in determining the applicable law.[227] Overall, the Federal Council also considered that it is justified, for economic reasons, to consider the secured creditor as the decisive person and that the parties to the pledge agreement are in a closer relationship with the law of the secured creditor's habitual residence than with the law of the claim.[228]

As legal scholars have pointed out, the criterion of the habitual residence of the secured creditor can be problematic with regard to dematerialisation of securities, in particular with tokens.[229] An advantage of tokens is that they can be easily transferred from one person to another. They are accordingly likely to be transferred frequently and circulate among persons. As they are dematerialised and only remain a type of book-entry instrument, it is difficult for a potential acquirer to determine whether a token is pledged or not.[230] However, the legislator did not consider this issue when amending art. 105 para. 2 of the PILA because it is still the law of the habitual residence of the secured creditor that applies, even though it might be highly difficult for an acquirer to

223 *Id.*, N 5.

224 *Id.*; Pius Fisch and Alexander Fisch, "Art. 105," in Pascal Grolimund, Leander D. Loacker, and Anton K. Schnyder (eds), *Basler Kommentar Internationales Privatrecht* (Helbing Lichtenhahn 2020), N 23.

225 Gaillard (n 209), N 5.

226 *Id.*

227 *Id.*

228 Message concernant une loi fédérale sur le droit international privé (loi de DIP), 10 November 1982, FF 1983 I 255 *et seq.*, 389: "pour des raisons économiques, il se justifie de considérer le créancier gagiste comme personne décisive et que les parties au contrat de gage sont dans un rapport plus étroit avec le droit de la résidence habituelle du créancier gagiste qu'avec le droit de la créance." See also Fisch and Fisch (n 224); Gaillard (n 209), N 5.

229 See Bahar (n 97), 20.

230 *Id.*

notice that a token has been pledged. As a result, third parties might be confronted by laws that were not possible to consider when acquiring a token. This situation leads to a dangerous legal uncertainty regarding the applicable law when acquiring a token. Moreover, the risk of legal uncertainty for third parties cannot be mitigated in practice by including a choice-of-law clause in the contract that establishes the pledge and choose the law that art. 145a of the PILA would designate as applicable, because the clause cannot be invoked against a third party in accordance with art. 105 para. 1 of the PILA.

Bahar argues that "against this backdrop, it would have been preferable, in my opinion, to rely on the general rule on the conveyance of rights or the rules applicable to the creation of security interests in so-called other rights which provide that the law applicable to the right itself governs the creation of security interests in such rights."[231] We agree with this author as it would have been advantageous for the issuer and the acquirer of a token, but seems in contradiction with the idea of the legislator that the secured creditor is the decisive person when a token is pledged. The rule based on this idea takes its roots in the Dispatch of the Federal Council of the PILA of 1983, at a time when the dematerialisation of securities had just begun. The Dispatch of the DLT Act, regrettably, did not even consider this issue when studying the possibility of modifying art. 105 para. 2 of the PILA specifically for tokens. It makes no differentiation with regard to conflict of laws between "a intangible instrument, negotiable instrument or an equivalent instrument," whereas it provides for a different solution for others' rights, such as intellectual property rights or parts of companies.[232] In our opinion, the legislator could also have made a distinction between intangible instruments, on the one hand, and negotiable as well as other instruments, on the other hand. As other instruments, the law applicable to tokens (potentially as defined in art. 145a para. 1 of the PILA) could have been chosen, similar to how art. 105 para. 2 last sentence of the PILA provides for so-called other rights. This could have led to a greater legal certainty for the third parties.

3.3.3 Lack of a Specific Provision for Pure Cryptocurrencies

The amendments to the PILA by the DLT Act focus on instruments that embed a claim against the issuer. Accordingly, they offer a conflict-of-laws framework for tokens stored on a distributed ledger that incorporate a claim. This is not the case for pure cryptocurrencies such as Bitcoin, which constitute a means of payment based on the principles of cryptography and are not issued by a

231 *Id.*

232 FF 2020 (n 105), 286.

central issuer against which a claim can be exercised.[233] Since no special rules have been adopted for such tokens, the general rules to determine the applicable law to the use of cryptocurrencies as instruments of payment remain applicable.[234]

We have shown that some legal uncertainties exist with regards to the conflict-of-laws rules applicable to cryptocurrencies.[235] By not having adopted a specific rule applicable to cryptocurrencies, the DLT Act does not provide a clear response to this question. When they have the opportunity, the courts will have to decide, and potentially bring nuances depending on the cryptocurrency in the case at hand. In the meantime, legal uncertainty remains, and parties cannot know for sure how cryptocurrencies will be treated from a Swiss PIL viewpoint. Bahar considers that such uncertainty may appear unsatisfactory, but in reality, it would offer flexibility and adaptability.[236] We agree with this opinion because cryptocurrencies are still developing in various forms. As outlined above,[237] there exists many different types of cryptocurrencies and tokens, which are highly different from one another. They will continue to evolve, so it is necessary and entirely justified to have not created a rule that could be outdated in the near future. In particular, cryptocurrencies could take new and unexperienced forms in Switzerland, such as a central bank digital currency (CBDC),[238] for which the rules of conflict-of-laws on money and means of payment may have to be adapted. With the approach followed by the legislator, the conflict-of-laws legal framework will be able to accommodate new developments, both on an international legal level and on a technical level. However, an immediate (but probably provisional) lack of legal certainty is the disadvantage of such an approach.

4 Concluding Remarks

By adopting the DLT Act, Switzerland positions itself at the forefront in the DLT sector and expresses its intention to welcome actors and companies active in

233 See *supra* sec. 3.2.1 with references in footnote 167.

234 Bahar (n 97), 20.

235 See *supra* sec. 2.2.2.2.

236 Bahar (n 97), 21.

237 See *supra* sec. 2.1.

238 On that subject, see David Chaum, Christian Grothoff, and Thomas Moser, "How to issue a central bank digital currency" (2021) 3 Swiss National Bank Working Papers 1, 1 et seq.; Mirjam Eggen and Cornelia Stengel, "Optionen zur rechtlichen Ausgestaltung von digitalem Zentralbankgeld (Wholesale CBDC)" (2020) 2 Gesellschafts- und Kapitalmarktrecht 200, 200 et seq.

this field by establishing a favourable legal environment. The DLT Act provides a comprehensive legal framework to include these technologies in an existing, well-established legal order. Despite the growing number of types of tokens, the approach of technological neutrality followed by the lawmakers allows the framework to cover many types of tokens, including types that do not exist yet.

This conclusion also holds true for the amendments to the PILA. The principles set forth by art. 145a of the PILA have a large scope of application and include most tokens. The conflict-of-laws solutions in this provision are in line with the general principles applicable to other rights. They grant considerable freedom to the issuer of a token to determine the governing law. Absent a choice of law, art. 145a para. 1 of the PILA sets forth subsidiary solutions based on the seat and the habitual residence of the issuer, which is consistent with conflict-of-laws principles known in contract law, company law and rights *in rem*. As a result, this approach does not require a complete paradigm change by creating a new type of digital asset and revolutionary rules entirely different from what was previously known.

However, this does not mean that the amendments are simply "old wine in a new bottle." This approach is reasonable and does not create an artificial split with the PIL principles that have proven efficient in practice and that are known among different jurisdictions. With the PIL aspects of the DLT Act, the recognised principles have simply been applied to tokens that may be exchanged through a DLT. Moreover the PILA, as amended by the DLT Act, does not regulate what should not be regulated at this early stage of the evolution of DLT, and in particular cryptocurrencies.

CHAPTER 23

Blockchain and Private International Law – The Perspective of the United States of America

Frank Emmert

1 Introduction

The United States usually approaches questions of Private International Law (PIL) quite differently from the rest of the world, in particular the Europeans, who have developed and refined the field for decades in a more collaborative and internationally coordinated way. First, problems such as choice of law or forum and the recognition and enforcement of foreign judicial decisions are discussed in the U.S. under the topic "conflict of laws." This label is actually more fitting since much of what the rest of the world calls PIL is really about the application of the rules ("laws") of one country versus those of another country ("conflict"). Moreover, there is really very little or no Private *International* Law at all. Instead, the respective rules are *national* rules about the application or recognition of laws or decisions of other nations, although they may have been adopted in implementation of an international convention.[1]

Second, the United States typically applies the same conflicts rules to their inter-state relations and to their inter-national relations. Thus, the question of whether Ohio or Illinois law should apply to a transaction and whether a Florida decision will be recognised and enforced in New York is, by and large, subject to the same rules that apply to the application of French versus Illinois

1 Various Hague conventions on the applicable law for sales contracts, agency, *etc.*, are examples of such conventions. However, even in the countries that have signed and ratified a particular convention, the convention itself is not normally applied directly by the courts. Instead, the national implementation law is applied, for example, the "Einführungsgesetz zum Bürgerlichen Gesetzbuch" in Germany (Einführungsgesetz zum Bürgerlichen Gesetzbuch in der Fassung der Bekanntmachung vom 21. September 1994 (BGBL. I S. 2494; 1997 I S. 1061), das zuletzt durch Artikel 3 des Gesetzes vom 21. Dezember 2021 (BGBL. I S. 5252) geändert worden ist) (German Introductory Act to the Civil Code) or the "Bundesgesetz über das Internationale Privatrecht (IPRG)" in Switzerland (Bundesgesetz über das Internationale Privatrecht (IPRG) vom 18. Dezember 1987 (Stand am 1. Januar 2022), RS 291) (Federal Act on Private International Law (PILA).

© FRANK EMMERT, 2023 | DOI:10.1163/9789004514850_025
This is an open access chapter distributed under the terms of the CC BY-NC-ND 4.0 license.

law and to the recognition and enforcement of an Australian judgment in New York. To make matters more complicated, those rules are mostly state laws – often based more on case law than on statutes – rather than federal law. As a consequence, there are literally some fifty-seven different sets of them,[2] and each forum typically applies their own. This makes it critically important whether a case is brought in court in New York – hence New York conflict rules will be applied – or maybe in California, where a different set of conflict rules may lead to different outcomes. Unsurprisingly, questions of jurisdiction of one court versus another have become a highly sophisticated art and science in the U.S.[3]

Third, due to a combination of sheer market size and widespread ignorance about foreign legal systems, American lawyers tend to apply American conflict rules and give little regard to the PIL of other nations. The same is true, almost as much, for the choice of substantive law. The attitude can often be summarised along the lines of "if you want to do business in our markets, you have to play by our rules."

Last but not least, the federal courts – including the Federal Supreme Court in Washington D.C. – do not have powers to oversee and harmonise state law, including state conflict rules. Even if a case about a transaction, *i.e.*, contract law, is brought in federal rather than in state court,[4] the federal court must apply the respective state conflict rules under the Erie doctrine.[5] This is different, however, if the parties litigate over a federal question, for example a decision of the Securities and Exchange Commission (SEC) in cryptocurrency matters. Those are not questions of state law, and the state courts do not have jurisdiction to hear disputes over federal questions.

Companies in the blockchain markets may face several scenarios. First, they may have a dispute with another private party, for example over a question of contract or employment law, tort liability, or real and personal property. These are all areas of state law and, in general, they belong to the jurisdiction of state

2 This includes the fifty states, the District of Columbia (Washington D.C.), Guam, Puerto Rico, the North Mariana Islands, Puerto Rico, Samoa, and the U.S. Virgin Islands.

3 Non-U.S. lawyers usually struggle to understand the intricacies of the U.S. system. An accessible summary can be found in Frank Emmert, *International Business Transactions – Text, Cases and Materials* (2nd edn, Carolina Academic Press 2020), in particular Part Six, Section 2 on Transnational Commercial Litigation, 697–860.

4 Parties have the right to initiate actions over state law, in particular contract law, directly in federal court, or to have a case removed from a state court to a federal court, if the disputing parties are from different states or countries *and* the amount in dispute is larger than US $75,000. This so-called "diversity jurisdiction" is codified in 28 U.S.C. § 1332(a) (2011).

5 See *Erie Railroad Co. v. Tompkins*, 304 U.S. 64 (1938).

courts.[6] Private parties may also have a dispute over a question of federal law, for example intellectual property rights. Those belong before federal courts. In disputes between two private parties, U.S. federal and state courts usually respect choice-of-law and forum clauses in the contracts. In the absence of agreement between the parties, a party can generally be sued in her own court, *i.e.*, at her domicile. Jurisdiction of a particular court is usually established by service of process, *i.e.*, formal delivery of a summons at the domicile or wherever a person can be found. This is important for foreign parties because they will be summoned before American courts if they can be served in the U.S., for example because they have a subsidiary or other physical premises, or even if they just happen to travel to the U.S. for business or pleasure.

Second, companies in the blockchain markets may have disputes with *federal* regulatory agencies like the SEC or the Commodities Futures Trading Commission (CFTC). If a dispute is initiated by a private party against a U.S. regulatory agency, it has to be filed in federal court at the seat of the agency. For the SEC and CFTC, this would be the U.S. District Court for the District of Columbia. If the agency is suing, it will also bring the lawsuit in U.S. federal court, even if the defendant is incorporated elsewhere. This so-called extraterritorial jurisdiction of U.S. courts will be further elaborated below.

Third, companies in the blockchain markets may have disputes with *state* regulatory authorities, for example the New York State Department of Financial Services, as the agency granting or denying the so-called BitLicense required for anyone wishing to "engage in any virtual currency business activity" in the State of New York, which includes buying or selling virtual currency in New York or in transactions with New York residents.[7]

For the purposes of the present overview, we can say that American private and public parties will typically succeed in bringing cases in U.S. federal or state courts even if the defendant is a foreign party. If jurisdiction and/or venue are contested, it is typically between courts in different states of the U.S. rather than American versus foreign courts. Anyone doing business in the U.S. – and the creation of a website that can be accessed by Americans may be sufficient for this qualification – has to be aware of the oversight powers and expansive jurisdiction of U.S. courts.[8]

---

6 The main exception to state jurisdiction of these state claims is diversity jurisdiction, outlined in (n 4).

7 For details, see Department of Financial Services, "Virtual Currency Businesses" (*New York State*) <https://www.dfs.ny.gov/virtual_currency_businesses> accessed 28 June 2023.

8 If a case is exceptionally litigated elsewhere, the foreign judgment will usually be recognised and enforced in the U.S. if three conditions are cumulatively met: first, the U.S. court requested to recognise and enforce the foreign judgment must have jurisdiction over the

Against this background, blockchain enterprises need to be more concerned with substantive regulations in the U.S. rather than trying to avoid the jurisdiction of American courts and regulatory authorities.

2 Blockchain and Cryptocurrency Regulation

Financial service providers have been heavily regulated and tightly supervised in most countries for decades. Banks, brokers, investment- and wealth advisors, stock- and commodity exchanges, insurance companies, and a whole range of other financial service providers require licenses to operate and must follow strict codes of conduct and reporting requirements. The reason is obvious: they are "trusted intermediaries," handling large amounts of their clients' money in transactions that are often opaque and hard to understand and track, both for the clients and the public authorities.

The possibility not only to record data in an immutable distributed ledger, but also to record transfers of value in the form of digital currencies on a blockchain, creates the perspective of direct or "peer-to-peer" transactions that cut out these trusted intermediaries. This is appealing, in particular to sophisticated clients and to those with a higher tolerance for the risk immanent in new technology, because the trusted intermediaries not only charge significant fees for their services but have also been subject to many scandals in the past, putting question marks on the "trusted" in trusted intermediaries.[9]

---

defendant, *i.e.*, service of process must be documented. Second, the country of origin of the judicial decision must be generally known to follow the rule of law and due process in judicial proceedings, and the defendant must not be able to show that procedural rights were violated in the particular case. Third, courts sometimes also require evidence that reciprocity is generally given, *i.e.*, the country of origin would also recognise and enforce U.S. judicial decisions if and when requested.

9 To name just a few, stock market regulations did not prevent Enron from manipulating its share valuations and causing investors losses of some US $74 billion; the WorldCom accounting fraud was not discovered until WorldCom stocks crashed from US $60 to US $1, causing losses of US $180 billion and thousands of jobs, sending the CEO to prison for 25 years; Bernie Madoff's hedge fund empire turned out to be a giant Ponzi scheme, and investors eventually lost US $64 billion; the 2008 financial crisis was caused primarily by mortgage originators and rating agencies slicing, dicing, and re-packaging sub-prime mortgages into investment grade securities that eventually collapsed and triggered a global recession; in 2021, German payment processor Wirecard collapsed after accounting fraud in multiple subsidiaries around Europe and the world was uncovered, and the German authorities initially investigated the whistleblowers and journalists instead of the fraudsters. The list could be expanded *ad nauseum*.

Of course, it would be naive to believe that financial markets will automatically be better off without trusted intermediaries and that peer-to-peer transactions will effectively eliminate the problems of the past. Any market with a capitalisation in excess of US $2 trillion[10] will attract its fair share of speculative investors, high-risk entrepreneurs, snake oil salesmen, and, more or less, organised crime. The technology behind blockchain and smart contract transactions is complex and poorly understood by most users, yet enormous amounts of money are already being invested and transacted on a regular basis,[11] and at least some participants have become fabulously wealthy in the process.[12] This creates an ideal environment for innovation and creativity but also for fraud, tax evasion, money laundering, crime and terrorism funding, and so on. For this very reason, regulators around the world are playing a game of catch-up with the developers and entrepreneurs in the crypto space. The crucial question is how to harness the technology, foster innovation and competition, attract high-tech jobs and services, and do so in a way that protects investors, developers, users, consumers, tax collectors, public safety, and the environment.

The challenge is exacerbated by the fact that the technology is built on the internet and accessible to anyone, regardless of national and jurisdictional borders. Blockchains and smart contracts are governed by code and follow the principles of offer and demand, whether or not these are in compliance with regulations applicable locally. As I have elaborated elsewhere,[13] the ideal and indeed the only truly sensible level for regulation of this technology is the international level, for example, in the form of a widely ratified and implemented convention developed and promoted by an agency such as the United Nations

10 As of 1 April 2022, the combined value of some 10,000 cryptocurrencies was in excess of US $2.2 trillion. At its recent peak in November 2021, this number reached beyond US $3 trillion. More importantly, developers of software and business applications in the blockchain space have been investing between US $1 and US $1.5 billion every month for several years, promising, and slowly bringing to market, a wide range of useful business ideas that may also be disruptive to certain traditional financial service providers.

11 The 24-hour transaction volume in cryptocurrencies regularly exceeds the US $100 billion mark.

12 Bitcoin, the most widely known digital currency, was launched in January 2009 and started trading in July 2010 at US $0.0008. In November 2021, it traded at more than US $68,000, at least for a while. An investor who put US $1,000 into bitcoin at the start and cashed out at the peak would have turned US $1,000 into a fortune of US $8.5 billion.

13 See Frank Emmert, "The Regulation of Cryptocurrencies in the United States of America" (*ResearchGate*, February 2022) <http://dx.doi.org/10.13140/RG.2.2.22099.66084> accessed 28 June 2023.

Commission on International Trade Law (UNCITRAL).[14] Such a convention should provide a list of requirements to be met by anyone wanting to issue coins or tokens, wanting to provide a marketplace for trading them, or wanting to develop business solutions for investors, commercial transactions, or consumer contracts. The convention should also provide for a variety of oversight mechanisms calibrated to the potential risks created by the different uses of the technology, as well as one centralised agency per country with meaningful resources and investigative powers. Importantly, the convention should provide a passport system, namely, that a crypto business lawfully operating in one signatory state can lawfully enter the markets in all other signatory states. The latter should only be allowed to interfere if they can show that a particular actor either obtained its licenses fraudulently from the home country, or, for reasons that may be specific to the host country, poses a real and substantial danger to non-economic or public interests of the host country – *e.g.*, the health and safety of its people, the protection of consumer financial interests, or the environment – and that those interests cannot be adequately protected by less severe restrictions or measures. Finally, the convention should provide for a dispute settlement system that is both accessible for the crypto businesses and effective, ideally along the lines of investor-state dispute settlement via international arbitration.[15]

Of course, the chances of drafting such a convention and convincing a sufficiently wide range of countries to ratify and effectively apply it are currently close to zero, in particular as views around the globe still differ fundamentally regarding the best way digital currencies should be managed

14 UNCITRAL already administers some very successful conventions in international business and trade, including the UN Convention on the International Sale of Goods (CISG) (UNCITRAL, *United Nations Convention on Contracts for the International Sale of Goods* (New York: United Nations Publications 2010) ("CISG"), and the UN Convention on the Recognition and Enforcement of Foreign Arbitral Awards (New York Convention) (UNCITRAL, *Convention on the Recognition and Enforcement of Foreign Arbitral Awards* (New York: United Nations Publications 2015) ("New York Convention"). For more information see United Nations, "Homepage" (*United Nations*) <https://uncitral.un.org/en> accessed 28 June 2023.

15 The regime developed for investor-state dispute settlement (ISDS) is unique because it allows international investors that have been expropriated or otherwise unlawfully injured by host countries to seek compensation in international arbitration proceedings. ISDS not only allows the investors to avoid the national courts of the host countries, where proceedings against the government might not always be promising, but it also produces arbitral awards that are enforceable in 169 countries and territories based on the New York Convention (n 14). For a detailed analysis, see Katia Yannaca-Small (ed), *Arbitration Under International Investment Agreements – a Guide to the Key Issues* (2nd edn, Oxford Univ. Press 2018).

or whether they should be allowed at all. In the absence of a global regulatory framework, the task falls on regulators at the national and regional level. What they should be doing is developing a coherent strategy that achieves the required safeguards while also providing legal certainty for the investors and developers and reliable information on what will be allowed, and on what conditions, in the foreseeable future. Furthermore, the national regulators should be in conversations with each other, exchange experiences, and facilitate mutual recognition of licenses granted to businesses in the blockchain space to facilitate international operations without the need – and the regulatory uncertainty – of seeking permits and registration in every country of operation. Let's see to what extent the regulators in the U.S. are following this advice.

3 Regulators and Regulations in the United States of America

Financial service providers are subject to a variety of regulations, requirements, and oversight by a number of different agencies and authorities in the U.S. At the federal level, the most important regulators and regulations are the following:

Under the Bank Secrecy Act (BSA),[16] so-called "money services businesses" (MSBs), which includes virtual currency businesses, must register with the Financial Crimes Enforcement Network (FinCEN), a bureau of the Department of the Treasury, using FinCEN Form 107.[17] Post registration, MSBs must:

- Establish effective BSA compliance programs;
- Establish effective customer due diligence systems and monitoring programs;
- Screen against Office of Foreign Assets Control (OFAC) and other government lists;
- Establish an effective suspicious activity monitoring and reporting process; and
- Develop risk-based anti-money laundering programs.[18]

The Federal Reserve (Fed), *i.e.*, the central bank of the U.S., and the Office of the Comptroller of the Currency (OCC), have oversight of banks and financial

16 See Office of the Comptroller of the Currency, "Bank Secrecy Act (BSA)" (*OCC*) <https://www.occ.treas.gov/topics/supervision-and-examination/bsa/index-bsa.html> accessed 28 June 2023.

17 FinCEN is the Financial Crimes Enforcement Network at the Department of the Treasury. The form, with explanations, can be found at <https://www.irs.gov/pub/irs-tege/fin107_msbreg.pdf> accessed 28 June 2023.

18 OCC (n 16). OFAC maintains lists of sanctioned countries, companies, and activities.

institutions to ensure their safety and soundness. Decentralised Finance or DeFi operators offering loan products and other services traditionally offered by banks may have to obtain a bank charter and follow regulations by the Fed and the OCC.[19]

The Securities and Exchange Commission (SEC) has qualified most cryptocurrencies and tokens as securities and, particularly, considers any ICO an issue of securities. Issuers and securities must be registered with the SEC and follow specific reporting requirements originally developed for publicly listed companies trading shares in the stock exchange.[20] Unregistered issuers may face cease-and-desist orders, disgorgement of profits, as well as civil penalties. From 2013 to 2022, the SEC issued more than US $2.6 billion in fines.

The Commodities Futures Trading Commission (CFTC) has qualified cryptocurrencies, such as bitcoin and ether, as commodities, and regulates trades and traders that are not executed immediately, *i.e.*, derivatives and futures trading by brokers and exchanges.[21] If cryptocurrency is locked by a buyer or customer in a smart contract for more than 48 hours and eventually released to the seller or service provider, the platform facilitating the transaction is probably engaged in futures trading and obliged to register with the CFTC. Like the SEC, the CFTC can pursue a number of enforcement strategies, including significant fines for unregistered exchanges, traders, brokers, and for misleading statements and practices.[22]

---

19 See Office of the Comptroller of the Currency, "What We Do" (*OCC*) <https://www.occ.treas.gov/about/what-we-do/index-what-we-do.html> accessed 28 June 2023. Among other laws and regulations, the Fed applies and enforces important parts of the Dodd Frank Wall Street Reform and Consumer Protection Act of 2010, Pub. L. 111–203, 124 Stat. 1376–2223.

20 The SEC applies and enforces, in particular, the Securities Act of 1933, Pub. L. 73–22, 48 Stat. 74, and the Securities Exchange Act of 1934, Pub. L. 73–291, 48 Stat. 881. However, the Investment Advisers Act of 1940, amended through Pub. L. 115–417, enacted 3 January 2019, the Sarbanes-Oxley Act of 2002, Pub. L. 107–204, 116 Stat. 745, the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, Pub. L. 111–203, 124 Stat. 1376–2223, and the Jumpstart Our Business Startups (JOBS) Act of 2012, Pub. L. 112–106, 126 Stat. 306, also contain important rules and procedures relevant for the work of the SEC. For details see Emmert (n 13), as well as Thomas Lee Hazen, *The Law of Securities Regulation* (8th edn, West Academic Publishing 2020).

21 The CFTC applies the Commodity Exchange Act of 1936, Pub. L. 74–675, 49 Stat. 1491 and other relevant laws. For the classification of cryptocurrencies as commodities, see U.S. Commodity Futures Trading Commission, "Bitcoin Basics" (*CFTC*) <https://www.cftc.gov/sites/default/files/2019-12/oceo_bitcoinbasics0218.pdf> accessed 28 June 2023.

22 For example, in October 2021, the CFTC imposed a fine of US $41 million against Tether for misleading statements that its stablecoin is fully backed by U.S. dollars. See U.S.

The Consumer Financial Protection Bureau (CFPB) protects consumers against unfair treatment and misleading advertising by banks, lenders, and other financial companies.[23]

The Federal Trade Commission (FTC) and the Commerce Department, together with the Department of Justice (DoJ) and the CFPB, are charged with the enforcement of antitrust legislation, protection against fraud, and protection of market access for consumers.

The Internal Revenue Service (IRS) at the Treasury Department is responsible for the assessment and collection of taxes on income and assets. It has classified cryptocurrencies as property rather than currency. As a consequence, if a user acquires a certain amount of crypto and sells it later at a higher price, the difference is subject to capital gains tax.

The Department of Justice has created a National Cryptocurrency Enforcement Team (NCET) to combat illicit activities involving cryptocurrencies. The DoJ collaborates in part and competes in part with the Federal Bureau of Investigation (FBI), the Department of Homeland Security (DHS), the U.S. Immigration and Customs Enforcement (ICE), and the U.S. State Department.

In addition to this cacophony of voices at the federal level, blockchain and cryptocurrency businesses are subject to various laws, regulations, and regulatory agencies at the state level. DeFi operators may hold or require state level bank charters. Money services businesses frequently have to register in every state where they operate. State attorney generals are responsible for the enforcement of consumer laws such as Unfair or Deceptive Acts and Practices (UDAP) laws. Importantly, some states like Wyoming have passed extremely

---

Commodity Futures Trading Commission, "CFTC Orders Tether and Bitfinex to Pay Fines Totaling $42.5 Million" (*CFTC*, 15 October 2021) <https://www.cftc.gov/PressRoom/PressReleases/8450-21> accessed 28 June 2023.

23 The CFPB is charged with the enforcement of the Consumer Credit Protection Act of 1968, Pub. L. 90–321, 82 Stat. 146, and in particular its Subchapters I (Truth in Lending Act "TILA"), II (Restrictions on Garnishments), IV (Equal Credit Opportunity Act, 15 U.S.C. §§ 1691–1691f), V (Fair Debt Collection Practices Act, Pub. L. 95–109, 91 Stat. 874 "FDCPA"), and VI (Electronic Funds Transfer Act, Pub. L. 95–630, 92 Stat. 3728 "EFTA"). The acts are broadly construed and cover any natural or legal persons regularly extending credit to consumers "in connection with loans, sales of property or services, or otherwise," including credit card issuers. DeFi operators and potentially other blockchain and cryptocurrency businesses are covered by at least some of these provisions.

welcoming legislation and registration requirements,[24] while other states like New York have created extremely restrictive rules and requirements.[25]

As a consequence, an operator like FTX US, seeking to be fully compliant, sought and obtained registration with FinCEN as an MSB, relied on Fenwick & West LLP for its BSA documentation and compliance program, was a registered and regulated commodity derivatives exchange and clearinghouse, held three licenses with the U.S. Commodity Futures Trading Commission (CFTC), implemented an extensive audit program for anti-money laundering (AML) compliance, maintained full US GAAP financial audit compliance with the help of Grant Thorton LLP, and was separately licensed in no fewer than 31 of the several states.[26]

---

24 Already in 2016, Wyoming declared digital currencies to be permissible investments (House Bill No. 0026, 16LSO-0050, 2016) and explicitly exempted "the transmission of monetary value and digital currency from the Wyoming Money Transmitter Act licensure requirements" (House Bill No. 0062, 16LSO-0019, 2016). In 2018, Wyoming made it clear that "a developer or seller of an open blockchain token shall not be deemed the issuer of a security," *i.e.*, "a person who develops, sells or facilitates the exchange of an open blockchain token is not subject to specified securities and money transmission laws," as long as the token is for consumptive purposes – *i.e.*, a utility token – and not marketed as an investment (House Bill No. 0070, 18LSO-0404, 2018). This directly contradicts the position of the SEC. Going further, Wyoming also exempted virtual currencies from State property taxes (Senate File No. 0111, 18LSO-0509, 2018). In 2019, Wyoming clarified that digital assets are property for the purposes of the UCC and provided a welcoming framework for custodial services for digital assets (Senate File No. 0125, 19LSO-0608, 2019). Issuers of utility tokens can do so in Wyoming by filing a "notice of intent." The fees for the notice amount to US $1,000 (House Bill No. 0062, 16LSO-0019, 2016). In 2020, the State further clarified how UCC Article 9 would apply to virtual currencies used as collateral in secured transactions (Senate File No. 0047, 20LSO-0198, 2020). In July 2021, the Wyoming Decentralized Autonomous Organization Supplement entered into force creating "a supplement to the Wyoming Limited Liability Company Act to provide law controlling the creation and management of a DAO." With this new law, Wyoming has absolutely broken new ground. It not only makes it the first jurisdiction anywhere in the world explicitly providing a legal basis for a DAO; it also provides the details that make the operation of such an organisation predictable and transparent.

25 See the New York BitLicense Regulation, 23 CRR-NY I 200 (2015) <https://govt.westlaw.com/nycrr/Browse/Home/NewYork/NewYorkCodesRulesandRegulations?guid=I7444ce8016961 1e594630000845b8d3e&originationContext=documenttoc&transitionType=Default&contextData=(sc.Default)&bhcp=1> accessed 28 June 2023. Its cumbersome and expensive registration and reporting requirements apply to anybody engaging in virtual currency business activity "involving New York or a New York Resident," *i.e.*, not just for businesses based in New York.

26 See West Realm Shires Services Inc., "Regulation and Licensure Information" (*FTX US*) <https://help.ftx.us/hc/en-us/articles/360046877253-Regulation-and-Licensure-Information> accessed 23 March 2023. There were additional states where FTX US could operate without having to be licensed. Since the crash of FTX, the website is no longer available. However, an archived version is available at <https://assets.website-files.com

The multitude of laws and regulations, registration requirements, administrative proceedings, investigations, decisions, executive orders, and other interpretative guidelines are, of course, subject to review by a multitude of courts at the federal and state level, and outcomes have not always been consistent, to say it politely.

Equally frustrating is the fact that none of this multitude of laws and regulations, registration, and other requirements, is able to warrant that a business model – crypto or not – is actually sound, nor do they prevent fraud and other diversion of funds by the owners/operators, as the recent spectacular collapse of the fully licensed exchange FTX has shown once again. This raises the question whether all these regulations and requirements, which impose very significant costs on startups, bring enough benefits to justify their existence. The U.S. authorities don't have such doubts, however, at least not yet.

4 Long-Arm Application of U.S. Regulations and the Implications for PIL

Between the SEC, the CFTC, and the DoJ, cease-and-desist orders are quite frequently issued, charges are filed, and civil and even criminal penalties are imposed against individuals and companies in the blockchain and cryptocurrency space. On average, this happens three to five times per month.[27] The frequency is bound to increase with the creation of cryptocurrency task forces at the SEC, DoJ, FBI, and the recent Executive Order of President Biden mandating more involvement and cooperation between more agencies.[28]

When reviewing proceedings against private businesses for issuing unregistered securities or trading in cryptocurrencies without SEC and/or CFTC registration, it is interesting to see that the U.S. authorities rarely distinguish between U.S.-based entities and entities and individuals outside of U.S. territorial jurisdiction. For example, in October 2020, the CFTC filed a complaint in court against multiple defendants, individuals and companies, jointly doing business under the BitMEX trademark, for violations of the Commodities Exchange Act.

/625f3cf193eb0bdbf6469cba/628eab2f96fde347cc283675_FTX%20Regulation%20and%20Licensure%20Information.pdf> accessed 28 June 2023.

27 The *Blockchain Law Alliance* is building a database for easy inter-institutional access to these proceedings. See Council on International Law and Politics, "Mission and Vision" (*CLIP*) <https://www.cilpnet.com/blockchain-law-alliance> accessed 28 June 2023.

28 President Joseph R. Biden, "Executive Order on Ensuring Responsible Development of Digital Assets" (*The White House*, 9 Mar 2022) <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/> accessed 28 June 2023.

The companies were incorporated in the Seychelles, Hong Kong, Bermuda, as well as Delaware. They operated the BitMEX cryptocurrency trading platform offering the trading of cryptocurrency derivatives on bitcoin, ether, litecoin, and others. BitMEX offered cryptocurrency derivatives, swaps, and futures to retail investors around the world, including in the U.S. However, the transactions were not executed on a registered board of trade, nor was BitMEX registered as a foreign board of trade with the CFTC. BitMEX also failed to implement a customer identification program in line with U.S. know-your-customer (KYC)[29] and anti-money laundering (AML)[30] requirements. To preempt a cease-and-desist order, as well as civil penalties, the defendants agreed not to execute any more futures contracts without CFTC registration, to implement adequate KYC and AML procedures, and to pay a civil monetary penalty of US $100 million.[31]

Just a few weeks before, the SEC charged Poloniex with operating an unregistered securities trading platform from 2014 to 2019. Although registered in Delaware, Poloniex LLC is a wholly-owned subsidiary of Circle Internet Financial Limited ("Circle"), an Irish private company. Poloniex accepted a cease-and-desist order, sold the platform, and agreed to "pay disgorgement of US $8,484,313.99, pre-judgment interest of US $403,995.12, and a civil money penalty of US $1,500,000, for a total of US $10,388,309.10," to the SEC.[32]

In September 2021, the SEC filed charges in the U.S. District Court, District of Massachusetts, against Rivetz International, a Cayman Island corporation, and

29 The Financial Crimes Enforcement Network (FinCEN) adopted the Customer Due Diligence Requirements for Financial Institutions ("CDD Rule"), last amended 2016 (see Customer Due Diligence Requirements for Financial Institutions, 81 Fed. Reg. 29398-29458 (11 May 2016) (amending 31 C.F.R. Parts 1010, 1020, 1023, 1024, and 1026) <https://www.gpo.gov/fdsys/pkg/FR-2016-05-11/pdf/2016-10567.pdf> accessed 28 June 2023). The CDD Rule "has four core requirements. It requires covered financial institutions to establish and maintain written policies and procedures that are reasonably designed to (1) identify and verify the identity of customers; (2) identify and verify the identity of the beneficial owners of companies opening accounts; (3) understand the nature and purpose of customer relationships to develop customer risk profiles; and (4) conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information." Financial Crimes Enforcement Network, "FinCEN Reminds Financial Institutions that the CDD Rule Becomes Effective Today" (*FinCEN*, 11 May 2018) <https://www.fincen.gov/news/news-releases/fincen-reminds-financial-institutions-cdd-rule-becomes-effective-today> accessed 28 June 2023.

30 FinCEN has authority to impose AML record keeping and reporting requirements based on the Bank Secrecy Act of 1970, Pub. L. 91–508, 84 Stat. 1118. Among others, transactions of US $10,000 or more have to be reported. See Financial Crimes Enforcement Network, "FinCEN's Legal Authorities" (*FinCEN*) <https://www.fincen.gov/fincens-legal-authorities> accessed 28 June 2023.

31 See *Commodity Futures Trading Commission v. HDR Global Trading Limited et al.*, No. 1:20-cv-08132-MKV (S.D.N.Y., 8 August 2021).

32 U.S. Securities and Exchange Commission, "SEC Charges Poloniex for Operating Unregistered Digital Asset Exchange" (*SEC*, 9 August 2021) <https://www.sec.gov/news/press-release/2021-147> accessed 28 June 2023.

its owner, a Massachusetts resident. The SEC accused the company of violating the securities registration provisions of Section 5 of the Securities Act of 1933. Between June and September 2017, Rivetz sold "RvT" digital tokens to more than 7,000 investors for a total of about US $18 million. Some 30% of the investors were in the U.S., but the ICO was not registered. The tokens were issued by Rivetz International from the Cayman Islands. The SEC is seeking injunctive relief, disgorgement of profits, and a civil penalty.[33]

In November 2021, the SEC filed a case against Terraform Labs PTE, Ltd., a South Korean company, and its owner and CEO Do Kwon, in New York. The filing states that the SEC "has reason to believe that Terraform Labs and Kwon participated in the creation, promotion, and offer to sell mAssets and MIR tokens to U.S. investors." The SEC had previously served investigative subpoenas on Terraform and Kwon in South Korea to obtain more information but the defendants refused to comply. The SEC is now seeking an order from the court to compel the production of the documents.[34]

The most interesting example of long-arm jurisdiction, however, is probably the Telegram case. In October 2019, the SEC filed an emergency action in New York "and obtained a temporary restraining order against two offshore entities conducting an [...] unregistered [...] digital coin offering in the U.S. and overseas that has [already] raised more than US $1.7 billion of investor funds."[35] The goal of the SEC was to stop the owners and operators of the Telegram Messenger app from continuing the sale of billions of digital tokens ("Grams") without having registered with the SEC. The case was filed in the U.S. District Court, S.D.N.Y., in spite of the fact that Telegram Group Inc. is a British Virgin Island corporation doing business out of Dubai, and TON, the issuer of the coins, is a BVI corporation operating out of Tortola and wholly owned by Telegram. The Telegram Messenger app has some 300 million users every month and is one of the most important communication tools on the internet. Since it offers end-to-end encryption for video chats and has no limits on file sharing, it has become a preferred tool for developers and investors in the cryptocurrency space, but also for hackers and other cybercriminals. The charges by the SEC against Telegram were eventually settled in June 2020. Telegram agreed to return US $1.2 billion to investors and pay a civil penalty of US $18.5 million.[36]

---

33 U.S. Securities and Exchange Commission, "SEC Charges Issuers and CEO for $18 Million Illegal Securities Offering" (*SEC* 8 September 2021) <https://www.sec.gov/litigation/litreleases/2021/lr25198.htm> accessed 28 June 2023.

34 U.S. Securities and Exchange Commission, "SEC Files Subpoena Enforcement Action Against Terraform Labs and Its CEO" (*SEC*, 12 November 2021) <https://www.sec.gov/litigation/litreleases/2021/lr25262.htm> accessed 28 June 2023.

35 *SEC v. Telegram Group Inc. and Ton Issuer Inc.*, No. 19-cv-09439 (S.D.N.Y. 26 June 2020).

36 *Id.*

Altogether, there are dozens of cases where the SEC or the CFTC have filed charges against non-U.S. entities simply because they were selling their digital assets or services without effectively excluding customers or investors from the U.S. In other words, U.S. authorities will exercise long-arm jurisdiction if a foreign entity is doing business in the U.S. or with U.S. parties without being fully registered.

This is not specific to the SEC and CFTC, either. The U.S. antitrust authorities have a long tradition of going after market manipulations done by foreign companies if they have "effects" inside the U.S.[37] As Najeeb Samie summarised, "[this] doctrine asserts that activities abroad, even those of foreign citizens, may be regulated because of their impact on interests within the territorial State's domain."[38]

In 2019, the United States Court of Appeals for the Tenth Circuit explicitly confirmed the SEC's authority to rely on a modified version of the effects doctrine when applying U.S. federal securities laws to conduct that occurred abroad.[39] Both the Securities Act of 1933 and the Securities Exchange Act of 1934 were amended by Sec. 929P of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010.[40] Sec. 22(c) of the Securities Act now provides as follows:

> Extraterritorial Jurisdiction – The district courts of the United States [...] shall have jurisdiction of an action or proceeding brought or instituted by the [Securities and Exchange] Commission or the United States alleging a violation of section 17(a) involving—
>
> – conduct within the United States that constitutes significant steps in furtherance of the violation, even if the securities transaction occurs outside the United States and involves only foreign investors; or
> – conduct occurring outside the United States that has a foreseeable substantial effect within the United States.[41]

37 The effects doctrine was effectively created by Judge Learned Hand in *United States v. Aluminum Co. of America*, 148 F.2d 416, 443 (2nd Cir., 1945).

38 Najeeb Samie, "The Doctrine of 'Effects' and the Extraterritorial Application of Antitrust Laws" (1982) 14 U. Miami Inter-Am. L. Rev. 23, 23. For comparative analysis see Roger P. Alford, "The Extraterritorial Application of Antitrust Laws: The United States and European Community Approaches" (1992–1993) 33 Va. J. Int'l L. 1.

39 *SEC v. Scoville,* 913 F.3d 1204 (10th Cir. 2019).

40 Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, Pub. L. 111–203, 124 Stat. 1376–2223. For the full text, see <https://www.cftc.gov/sites/default/files/idc/groups/public/@swaps/documents/file/hr4173_enrolledbill.pdf> accessed 28 June 2023.

41 *Id.*, Section 17(a) makes it "unlawful for any person in the offer or sale of any securities [...] (1) to employ any device, scheme, or artifice to defraud, or (2) to obtain money or property

In effect, this gives powers to the SEC over foreign natural and legal persons in two cases: if there was some conduct within the U.S., or if there is a "foreseeable substantial effect" within the U.S. In practice, the SEC always sees a "foreseeable substantial effect" if securities created outside of the U.S. are available to purchasers from the U.S. and have actually been purchased by a number of U.S. persons.[42] Importantly, since websites advertising an ICO or other issue of cryptocurrency, including utility tokens, are generally available from anywhere, and since issuers have an obligation to conduct KYC procedures before selling digital assets to a client, foreign companies cannot claim that they were unaware of the fact that their coins or tokens were purchased by persons domiciled in the United States.

As the growing number of cases shows, the SEC is by no means shy in using these powers, and unless the foreign entities are willing to be permanently excluded from doing business in the U.S. or visiting or otherwise interacting with the U.S., the SEC is also able to enforce its decisions.

5 Conclusions and Recommendations

Natural and legal persons selling digital assets, whether they are coins with broad application, utility tokens that can only be used to acquire goods or services from the issuer, or non-fungible tokens (NFTs), as long as the digital

---

by means of any untrue statement of a material fact or any omission to state a material fact necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; or (3) to engage in any transaction, practice, or course of business which operates or would operate as a fraud or deceit upon the purchaser." A parallel provision for extraterritorial jurisdiction is included in Sec. 27(b) of the Securities Exchange Act of 1934, Pub. L. 73–291, 48 Stat. 881.

42 In one case, the SEC – supported by the Federal Court of Appeals, 2nd Circuit – deemed it enough that *one single American* had been able to purchase the respective coins, in spite of the fact that the issuer had clearly announced that U.S. residents were not eligible to participate in the ICO, see *Barron v. Helbiz*, Inc., No. 1:20-cv-04703, 2021 WL 229609 (S.D.N.Y. Oct. 4, 2021). In this case, the SEC had originally and seriously argued that its jurisdiction over an ERC20-token sale was established merely by the fact that a significant number of nodes running the Ethereum blockchain are located in the U.S., i.e. that some of the bits and bytes or the electrons used in the ICO were passing through American cyberspace, see *id.*, at 4. As anyone with even just rudimentary understanding of blockchain technology and the internet will appreciate, this argument, if successful in court, would give the SEC authority over any activities anywhere in the world, using Ethereum or the Ethereum blockchain, and probably most other blockchains as well.

For further analysis see Frank Emmert, "The Long Arm of the SEC in the Regulation of Digital Currencies", forthcoming in the Indiana Int'l & Comparative Law Review 2023; draft available on ResearchGate.

assets are tradeable and their value is expected to appreciate, have precisely two choices: They can either register with the SEC and FinCEN, and potentially the CFTC, or they have to effectively *and completely* block U.S. persons from purchasing those assets.

Registration as a money services business with FinCEN is relatively straightforward and imposes only internal expenses for the applicant.[43]

Registration with the CFTC will only be necessary if cryptocurrency futures or derivatives are being offered or if the foreign company wants to deliver broker services, become a commodity pool operator, or a commodity trading advisor.[44]

At the SEC, there are multiple options. Prospective issuers of securities generally have to register with the SEC pursuant to Sections 6 to 8 of the Securities Act,[45] using Form S-1,[46] as if they were preparing to sell common stock in the U.S., unless they fall under one of the exemptions. Form S-1 must be accompanied by a prospectus that meets the requirements outlined in Sec. 10 of the Act and the Form itself.[47] Extensive annexes with exhibits pursuant to 17 CFR § 229.601[48] and financial statements pursuant to 17 CFR Part 210[49] are also required, which makes the registration complex and costly. Once Form S-1 is filed, the SEC engages in a complex review procedure, typically involving a back-and-forth of questions and clarifications with the applicant. Pursuant to

43 See Financial Crimes Enforcement Network, "BSA E-Filing System" (*FinCEN*) <https://bsaefiling.fincen.treas.gov/Benefits.html> accessed 28 June 2023.

44 <https://www.cftc.gov/International/ForeignMarketsandProducts/foreignprodsales.html#:~:text=As%20set%20forth%20in%20CFTC,an%20exemption%20from%20registration%20under> accessed 28 June 2023.

45 Securities Act of 1933, Pub. L. 73–22, 48 Stat. 74. For the full text, see <https://www.govinfo.gov/content/pkg/COMPS-1884/pdf/COMPS-1884.pdf>. For details, see Marc Steinberg, *Understanding Securities Law* (7th edn, Carolina Academic 2018), 125–152, 51–124.

46 Securities and Exchange Commission, "Form S-1: Registration Statement Under the Securities Act of 1933" (*SEC*) <https://www.sec.gov/files/forms-1.pdf> accessed 28 June 2023.

47 "In the prospectus, the 'issuer' of the securities must describe in the prospectus important facts about its business operations, financial condition, results of operations, risk factors, and management. It must also include audited financial statements." See American Bar Association, "What Constitutes a Security and Requirements Relating to the Offer and Sales of Securities and Exemptions From Registration Associated Therewith" (*ABA*, 27 April 2017) <https://www.americanbar.org/groups/business_law/publications/blt/2017/04/06_loev/> accessed 28 June 2023.

48 17 CFR § 229.601. For the full text, see Cornell Law School, "17 CFR § 229.601 – (Item 601) Exhibits" (*Legal Information Institute*) <https://www.law.cornell.edu/cfr/text/17/229.601> accessed 28 June 2023.

49 17 CFR Part 210. For the full text, see Cornell Law School, "17 CFR Part 210 - Form and Content of and Requirements for Financial Statements, Securities Act of 1933, Securities Exchange Act of 1934, Investment Company Act of 1940, Investment Advisers Act of 1940, and Energy Policy and Conservation Act of 1975" (*Legal Information Institute*) <https://www.law.cornell.edu/cfr/text/17/part-210> accessed 28 June 2023.

Sec. 5, securities can only be issued after the SEC has declared the registration "effective." Once an IPO or ICO is completed, there are various disclosure and regular filing requirements for as long as the company remains in business.[50]

Several exemptions for issuers of securities can be of interest in the context of cryptocurrency businesses and ICOs. Rule 506 of Regulation D – the Exemption for Limited Offers and Sales Without Regard to Dollar Amount of Offering[51] – provides two exemptions that can be used by issuers of securities. The first option is Rule 506(b). A company relying on this exemption can sell an unlimited number of securities to "accredited investors"[52] and to up to thirty-five non-accredited investors.[53] Under this Rule, however, the company is not allowed to market or advertise an ICO to the public. The second option is Rule 506(c). A company relying on this exemption can market and advertise an ICO but sell only to accredited investors. The company has to verify the status of the investors; for example, by reviewing bank and brokerage statements. Under both options, the securities are restricted. They cannot be re-sold for six months or up to a year unless they are being registered. Moreover, a company wanting to avail itself of Rule 506 needs to file a Form D with the SEC after selling securities. In this Form it must disclose details about the company. Lastly, the offering for sale of the securities most likely also must be filed with various regulators at the level of the several states.

Regulation A+ was created by the SEC based on a mandate in the Jumpstart Our Business Startups (JOBS) Act of 2012 to make it easier for startup companies to conduct crowdfunding and certain limited public offerings as an

50 For additional details, *see* Steinberg (n 45), 153 et seq.

51 17 CFR § 230.506. For the full text, see Cornell Law School, "17 CFR § 230.506 - Exemption for limited offers and sales without regard to dollar amount of offering" (*Legal Information Institute*) <https://www.law.cornell.edu/cfr/text/17/230.506> accessed 28 June 2023.

52 Accredited investors are natural persons with "earned income that exceeded US $200,000 (or US $300,000 together with a spouse or spousal equivalent) in each of the prior two years, and reasonably expects the same for the current year, OR has a net worth over US $1 million, either alone or together with a spouse or spousal equivalent (excluding the value of the person's primary residence), OR holds in good standing a Series 7, 65 or 82 license." Securities and Exchange Commission, "Accredited Investors – Updated Investor Bulletin" (*Investor.gov*, 14 April 2021) <https://www.investor.gov/introduction-investing/general-resources/news-alerts/alerts-bulletins/investor-bulletins/updated-3> accessed 28 June 2023. The respective licenses are financial professional licenses obtained after an examination by the Financial Industry Regulatory Authority (Series 7 and 82) or the North American Securities Administrators Association (NASAA) (Series 65). A trust with assets in excess of US $5 million and certain other legal persons can also be accredited investors.

53 Even the non-accredited investors must be "financially sophisticated;" for more information see Securities and Exchange Commission, "Investor Bulletin: Private Placements Under Regulation D" (*SEC*, 24 September 2014) <https://www.sec.gov/oiea/investor-alerts-bulletins/ib_privateplacements.html> accessed 28 June 2023.

alternative to a full-scale IPO.[54] Regulation A pre-dated the JOBS Act but was limited, after the most recent amendment in 1992, to offerings of a maximum of US $5 million. Based on the JOBS Act, the limit was initially raised to US $50 million in 2015. Since 2021, small and medium sized businesses and entrepreneurs have a choice between Tier 1 (offerings up to US $20 million) and Tier 2 (offerings up to US $75 million). Only companies incorporated in the United States or Canada can avail themselves of this exemption. However, an incorporation in the U.S. is not difficult to achieve for foreign natural or legal persons.

Both Tiers allow public solicitations. In a Tier 2 offering, securities can only be sold to accredited investors or to natural or legal persons who meet certain income criteria.[55] For both types of offerings, the issuer must file Form 1-A with the SEC.[56] For Tier 2, the requirements of the filing are stricter. Another important detail is that a Tier 1 offering does not preempt state registration and qualification requirements. By contrast, an offering filed with the SEC under Tier 2 does preempt state restrictions or requirements.[57]

The Tier 2 exemption in Regulation A+ is an attractive alternative to a regular filing with the use of Form S-1, in particular since the issuer need not concern herself with parallel requirements at the state level. However, even under Regulation A+, the procedure is complicated, time consuming, and costly. As a result, it will rarely be worthwhile for a company to go through this procedure unless the issuer is planning – and confident – to sell securities for at least US $3–5 million in the United States.[58]

---

54 For detailed analysis see David N. Feldman, *Regulation A+ and Other Alternatives to a Traditional IPO: Financing Your Growth Business Following the JOBS Act* (John Wiley & Sons 2018).

55 §230.251(d)(2)(i)(C) provides that "the aggregate purchase price to be paid by the purchaser for the securities (including the actual or maximum estimated conversion, exercise, or exchange price for any underlying securities that have been qualified) is no more than ten percent (10%) of the greater of such purchaser's: (1) Annual income or net worth if a natural person (with annual income and net worth for such natural person purchasers determined as provided in Rule 501 (§ 230.501)); or (2) Revenue or net assets for such purchaser's most recently completed fiscal year end if a non-natural person." 17 CFR § 230.251. For the full text, see Cornell Law School, "17 CFR § 230.251- Scope of exemption" (*Legal Information Institute*) <https://www.law.cornell.edu/cfr/text/17/230.251> accessed 28 June 2023.

56 Securities and Exchange Commission, "Form 1-A Regulation A Offering Statement Under the Securities Act of 1993" (*SEC*) <https://www.sec.gov/files/form1-a.pdf> accessed 28 June 2023.

57 Facilitating Capital Formation and Expanding Investment Opportunities by Improving Access to Capital in Private Markets, 86 Fed. Reg. 3496–3605 (14 January 2021) <https://www.federalregister.gov/documents/2021/01/14/2020-24749/facilitating-capital-formation-and-expanding-investment-opportunities-by-improving-access-to-capital> accessed 28 June 2023.

58 Specialised law firms like Bull Blockchain Law LLC in Philadelphia can prepare a Reg A+ filing at a cost of approximately US $100,000.

CHAPTER 24

A German Approach: *Lex Supervisionis Registri* and Subordinate Connecting Factors

Felix M. Wilke

1 Introduction: The Blockchain Strategy by the Federal Government

The 2018 coalition agreement between the governing parties (Christian and Social Democrats: CDU, CSU and SPD) included the aim of strengthening Germany's position with regard to digitalisation and financial technology (FinTech).[1] It specifically addressed blockchain technology, with a comprehensive blockchain strategy to be developed by the Federal Government. The strategy was then published in September 2019.[2] It envisions 44 measures in five areas: blockchain in the finance sector; advancing innovative projects and regulatory sandboxes, for example in the energy sector; clear and reliable frameworks for investments (in particular with regard to data protection or company law); digitising services of public administration such as digital identities; distributing information.[3] Cross-border situations do not figure prominently in the Blockchain Strategy.[4] The issue of the applicable law is discussed only once and in passing, in the context of a potential international arbitration authority.[5]

1 Koalitionsvertrag zwischen CDU, CSU und SPD, p. 44/70 et seq.: Die Bundesregierung, "Coalition agreement between CDU, CSU and SPD" <https://www.bundesregierung.de/breg-de/themen/koalitionsvertrag-zwischen-cdu-csu-und-spd-195906> accessed 28 June 2023.

2 Bundesministerium für Wirtschaft und Klimaschutz (BMWK) and Bundesministerium der Finanzen, "Blockchain Strategy by the Federal Government: We Set Out the Course for the Token Economy" (*BMWK*, 18 September 2019) <https://www.bmwk.de/Redaktion/EN/Publikationen/Digitale-Welt/blockchain-strategy.pdf?__blob=publicationFile&v=3> ("Blockchain Strategy") accessed 28 June 2023.

3 In this regard, see the Digital Hub Initiative: BMWK, "Twelve Hubs, One Digital Ecosystem" (*BMWK*) <https://www.de-hub.de/en/> accessed 28 June 2023.

4 Blockchain Strategy (n 2), 12, 18. References to international cooperation and the development of international standards abound, however.

5 *Id.*, 13 ("new challenges from the legal viewpoint, for instance on the matter of which legal system is applied").

© FELIX M. WILKE, 2023 | DOI:10.1163/9789004514850_026
This is an open access chapter distributed under the terms of the CC BY-NC-ND 4.0 license.

A 2020 study by Bitkom[6] showed that Germany had started implementing most of the proposed measures although, in some areas, the connection to blockchain was not obvious.[7] Germany does not (yet?) have specific blockchain legislation, however, nor does the word "blockchain" appear in any piece of legislation. Accordingly, there is no special blockchain conflicts rule. Nonetheless, the 2021 e-Securities Act was clearly designed with blockchain technology in mind. A considerable portion of this contribution thus pertains to this Act and its conflicts provision (*infra* 2). An analysis of the suitability of the provision for other blockchain issues and of existing or potential alternatives follows (*infra* 3).

2 The Example of § 32 of the e-Securities Act

The e-Securities Act comes with its own conflicts rule in § 32. This section first addresses general features of the e-Securities Act including its relevance in the blockchain context (*infra* 2.1). It then turns to the conflicts issues in particular, analysing § 32 of the e-Securities Act[8] against the backdrop of existing German conflicts rules for (electronic) securities (*infra* 2.2).

2.1 *General Information about the e-Securities Act*

The e-Securities Act (*Gesetz über elektronische Wertpapiere* (*eWpG*)) was itself part of the larger Act Introducing e-Securities of June 3, 2021.[9] It entered into force a week later on June 10, 2021. The Act Introducing e-Securities also modified certain other Acts pertaining to capital markets with regard to e-securities, among them the Securities Account Act (*Depotgesetz*), the Securities Prospectus Act (*Wertpapierprospektgesetz*), the Banking Act (*Kreditwesengesetz*), the Supervision of Financial Services Act (*Finanzdienstleistungsaufsichtsgesetz*) and the Capital Investment Code (*Kapitalanlagegesetzbuch*). The creation of

6 Bitkom is an association under German law representing more than 2,000 companies in the context of the digital economy. See Bitkom, "About us" <https://www.bitkom.org/EN/About-us/About-us.html> accessed 28 June 2023.

7 Bitkom, "Bestandsaufnahme: Ein Jahr Blockchain Strategie der Bundesregierung (Infopapier)" (*Bitkom*, 2020) <https://www.bitkom.org/sites/main/files/2020-09/200928_umsetzungsstand_blockchain-strategie.pdf> accessed 28 June 2023.

8 Also see: Felix M. Wilke, "Das IPR der elektronischen Wertpapiere" (2021) 41 Praxis des Internationalen Privat- und Verfahrensrechts 502.

9 Gesetz über elektronische Wertpapiere (eWpG), Federal Law Gazette I 29/2021, 1423 ("eWpG").

a legal framework for electronic securities means the implementation of the very first measure provided for in the Blockchain Strategy.[10]

2.1.1 Overview of the Act

The e-Securities Act has seven sections with a total of 33 provisions. Its substantive scope is limited to bearer bonds (§ 1 of the e-Securities Act).[11] This is to be read as an exclusion of electronic shares in particular.[12] The act is a mixed instrument in that it contains rules of both public law and private law. On the public law side, there is, for example, the duty to notify the supervisory authority of having established a central register before starting to make any records in the register (§ 12(3) of the e-Securities Act) or to arrange for the publication of certain information in the Federal Gazette (§ 20 of the e-Securities Act). While § 11 of the e-Securities Act provides for the supervision of the maintenance of e-securities registers by the Federal Financial Supervisory Authority (*Bundesanstalt für Finanzdienstleistungsaufsicht* (*BaFin*)), § 31 of the e-Securities Act contains a long list of administrative offences, to be sanctioned by penalties up to € 100,000.

With regard to private law, the Act sets forth, *inter alia*, formal requirements for e-securities (§ 2(1) e-Securities Act). It also deals with different questions concerning dispositions about a subset of e-securities,[13] such as the conditions for acquisition of ownership of e-securities including the possibility of acquiring ownership of an e-security in good faith (§ 25 *et seq.* of the e-Securities Act). As, under German law, one generally can only be the owner of things, *i.e.* corporeal objects (§ 90 Civil Code), § 2(3) of the e-Securities Act provides for the legal fiction that e-securities are things. Hence, but for special provisions, the general rules of German private law about rights *in rem* apply to e-securities. One main consequence is that a person with a right *in rem* in e-securities enjoys special protection in insolvency (§ 47 Insolvency Act) and enforcement situations (§ 771 Code of Civil Procedure).[14] In terms of Private International

10 Blockchain Strategy (n 2), 6; *supra* sec. 1.

11 But see *infra* sec. 2.2.4 for the scope of application of the conflicts rule.

12 Draft by the Government for an Act Introducing e-securities, Bundestag-Drucksache ("BT-Drs.", Parliamentary Document) 19/26925, 38 ("Government Draft").

13 E-securities in an individual recording, *infra* sec. 2.1.2. On the issue of dispositions in general see Matthias Casper, "§ 28 Elektronische Schuldverschreibungen," in Florian Möslein and Sebastian Omlor (eds), *FinTech-Handbuch* (München: C.H. Beck 2021), paras. 40–56; Sebastian Omlor, "Elektronische Wertpapiere nach dem eWpG" (2021) Recht Digital 371, 375–76.

14 See only Matthias Lehmann, "Das Gesetz zur Einführung von elektronischen Wertpapieren" (2021) 74 Neue Juristische Wochenschrift 2318, 2320.

Law (PIL), however, recourse to the usual rules for rights in *rem*[15] is not necessary in principle, as there are special provisions.[16]

2.1.2 The Types of e-Securities, of e-Security Registers, and of Recording the Bearer

Some distinctions under substantive law deserve special attention in light of their relevance for PIL and/or blockchain technology. First, the e-Securities Act provides for two types of registers: Central registers (§ 12 *et seq.* of the e-Securities Act) and crypto-securities registers (§ 16 *et seq.* of the e-Securities Act; more on them in the following section). Only central securities depositories and depositary banks can maintain a central register (§ 12(2) of the e-Securities Act). In this regard, the main difference to current practice seems to be the abandonment of the need to store any type of paper document. By contrast, any natural or legal person or partnership with legal personality can theoretically maintain a crypto-securities register (after authorisation by the German Federal Financial Supervisory Authority[17]).[18] The e-Securities Act refers to the person maintaining a register as the "register office" (*registerführende Stelle*). The term, much less ambiguous in German, thus should not be misunderstood to imply some government-run agency.

Second, the e-Securities Act distinguishes between two types of e-securities, depending on the type of register in which an e-security is recorded. If recorded in a central register, it is a "central register security" (§ 4(2) of the e-Securities Act) – if recorded in a crypto-securities register, it is a "crypto-security" (§ 4(3) of the e-Securities Act). Only the latter type of security (register) is relevant for the blockchain context.[19]

Third, there are two ways to record the bearer of e-securities. For one, a central securities depository or a depositary bank can be recorded as the bearer (only). This is called a "collective recording" (*Sammeleintragung*), § 8(1) No. 1 of the e-Securities Act. For another, a natural or legal person or partnership with legal personality can be recorded as the bearer of the e-security who also enjoys the legal position documented by the e-security. Pursuant to § 8(1) No. 2 of the e-Securities Act, this constitutes an "individual recording" (*Einzeleintragung*). This third distinction is, in theory, independent from the first two. In

15 *Infra* sec. 2.2.2.

16 *Infra* sec. 2.2.3 et seq.

17 Maintaining a crypto-securities register is a financial service pursuant to § 1(1a) cl. 2 No. 8 Banking Act, and carrying out financial services in Germany, in principle, requires authorisation (§ 32(1) cl. 1 Banking Act) (Kreditwesengesetz – KWG).

18 Government Draft (n 12), 60.

19 *Infra* sec. 2.1.3.

other words, both types of recordings can be made in both types of registers (and thus for both types of e-securities).[20] It is to be assumed, however, that collective recordings will prevail in central registers and individual recordings will prevail in crypto-securities registers.[21]

2.1.3 The Relevance of the Act for Blockchain

It should be noted that the e-Securities Act is not a genuine piece of blockchain legislation. It does not deal with distributed ledger technology as such. The Act does not require the recording of e-Securities in a blockchain, nor will just any type of blockchain fulfill the requirements of the Act. What is more, the idea of e-securities in a *central* register[22] obviously clashes with the principles of *distributed* ledger technology (DLT).

On the other hand, the Act is far from oblivious to blockchain. Crypto-securities registers[23] are supposed to be "forgery-proof"[24] recording systems in the form of decentralised pools into which data is entered chronologically and in which data is protected against illicit deletion and subsequent modification (§§ 16(1), 2(11) of the e-Securities Act). The combination of a decentralised structure, chronology, and the protection against forgery, deletion, and modification sounds a lot like blockchain. It comes as no surprise, then, that the proposal for the Act singled out DLT in this context.[25] "Blockchain" also figures very prominently at the very beginning of the proposal as a potential medium to be used for e-securities.[26] Both permissioned and permissionless blockchains[27] could meet the requirements of the Act.[28] By not expressly referring to blockchain or any other particular technology, *i.e.* by assuming a

20 Government Draft (n 12), 49.

21 Casper, "§ 28 Elektronische Schuldverschreibungen," para. 22.

22 *Supra* sec. 2.1.2.

23 *Id.*

24 This can hardly mean "entirely forgery-proof," as (even) the blockchain could be subject to manipulations, *e.g.* Dimitrios Linardatos, "Elektronische Schuldverschreibungen auf den Inhaber – des Wertpapiers neue Kleider" (2020) 32 Zeitschrift für Bankrecht und Bankwirtschaft 329, 335; Michèle Finck, *Blockchain Regulation and Governance in Europe* (Cambridge: Cambridge University Press 2019), 30. Indeed, the term is to be understood merely as "secured against forgeries" in line with the state of the art; see Government Draft (n 12), 59.

25 Government Draft (n 12), 42 and 59.

26 *Id.*, 1.

27 As to the distinction, *e.g.*, Markus Kaulartz, "§ 5 Blockchain-Technologien," in Florian Möslein and Sebastian Omlor (eds), *FinTech-Handbuch* (München: C.H. Beck 2021), para. 40.

28 Government Draft (n 12), 60.

technologically neutral position, the legislator wanted the e-Securities Act to be able to accommodate future developments.[29]

2.2 *The Conflicts Rule of the e-Securities Act*

In addition to the provisions of public and substantive private law outlined above, § 32 of the e-Securities Act sets forth the following conflicts rule:

> **§ 32 Applicable Law**
> (1) To the extent that § 17a Securities Account Act does not apply, rights regarding an e-security and dispositions about an e-security are governed by the law of the State under whose supervision the register office is in whose e-securities register the e-security is recorded.
> (2) If the register office is not under supervision, its seat is decisive. If the seat of the register authority cannot be determined, the seat of the issuer of the e-security is decisive.[30]

2.2.1 German Conflicts Doctrine for Securities in a Nutshell

In substantive German private law, securities thus far had to be recorded in a piece of paper: the German word "Wert*papier*" itself implies a piece of paper – making the very idea of an electronic "Wertpapier" an oxymoron.[31] From this followed a central distinction with regard to securities between the right deriving from the piece of paper and the right in the piece of paper.[32] The former is the documented right. It might be a share under company law, a claim under the law of contractual obligations, or a right *in rem*. The latter is the legal position with regard to the document itself, in particular: ownership of the piece of

29 *Id*., 29.

30 The official German version of the eWpG (n 9) reads: "§ 32 Anwendbares Recht (1) Soweit nicht § 17a des Depotgesetzes anzuwenden ist, unterliegen Rechte an einem elektronischen Wertpapier und Verfügungen über ein elektronisches Wertpapier dem Recht des Staates, unter dessen Aufsicht diejenige registerführende Stelle steht, in deren elektronischem Wertpapierregister das Wertpapier eingetragen ist.

(2) Steht die registerführende Stelle nicht unter Aufsicht, so ist der Sitz der registerführenden Stelle maßgebend. Ist der Sitz der registerführenden Stelle nicht bestimmbar, so ist der Sitz des Emittenten des elektronischen Wertpapiers maßgebend."

31 Lehmann (n 14), 2318 fn 2; Matthias Lehmann, "Zeitenwende im Wertpapierrecht: Der Referentenentwurf für ein Gesetz über elektronische Wertpapiere (eWpG)" (2020) 20 Zeitschrift für Bank- und Kapitalmarktrecht 431, 433.

32 Christiane Wendehorst, "Art. 43 EGBGB," in Franz J. Säcker et al. (eds), *Münchener Kommentar zum BGB* (München: C.H. Beck 2021), para. 200; Heinz-Peter Mansel, "Anhang zu Art. 43 EGBGB," in *J. von Staudingers Kommentar zum Bürgerlichen Gesetzbuch* (Berlin: de Gruyter 2015), para. 23.

paper. Whether a change concerning one of these rights implicates a change for the other depends on the type of security. For some, the right deriving from the piece of paper follows the right over the piece of paper. For example, any new owner of the piece of paper would, in principle, also be the new creditor. For other securities, it works just the other way around. Thus, a person who has acquired the legal position documented in the piece of paper would have become the owner of the piece of paper at the same time, giving that person a claim for delivery against the possessor of the piece of paper.

German conflicts doctrine for securities adheres to the same distinction. Therefore, one needs to separate the law applicable to the right documented in the piece of paper (*Wertpapier*rechts*statut*) from the law applicable to the right regarding the piece of paper (*Wertpapier*sach*statut*).[33] The former is determined using the conflicts rules of the respective field, *i.e.* conflicts rules for companies concerning a documented share, conflicts rules for contractual obligations concerning a documented contractual obligation, or conflicts rules for rights *in rem* concerning a documented right *in rem*. The latter, *i.e.* the law applicable to the right regarding the piece of paper, is always determined by conflicts rules for rights *in rem*.

Crucially, German doctrine considers the law applicable to the right deriving from the piece of paper as "dominant."[34] Whether or not a piece of paper is to be considered a security in the first place and whether or not the documented legal position is connected to the legal position with regard to the piece of paper is subject to the law applicable to the right deriving from the piece of paper.

2.2.2 § 32 of the e-Securities Act in the Context of German PIL

The main source of Germany's domestic[35] conflicts rules is the Introductory Act to the Civil Code (EGBGB). This Act is not a pure PIL instrument, but includes, among others, rules of intertemporal private law, rules on the relationship of federal and state law, and details on a business's duty of information *vis-à-vis* consumers.[36] Issues of international civil procedure are addressed by different

33 For a short account in English: Gerald Spindler, "Fintech, digitalization, and the law applicable to proprietary effects of transactions in securities (tokens): a European perspective" (2019) 24 Uniform Law Review 724, 728–29; Wendehorst (n 32); Mansel (n 32).

34 Wendehorst (n 32), para. 201; Mansel (n 32), paras. 24–25.

35 In particular: not determined by the EU legislator. Of course, EU conflicts rules are highly relevant in Germany, *infra* sec. 3.1.

36 For more background on the conflicts rules in the EGBGB in English see Felix M. Wilke, *A Conceptual Analysis of European Private International Law*: *The General Issues in the EU and Its Member States* (Cambridge, Antwerp, Chicago: Intersentia 2019), 58–60.

acts, the most important being the German Code of Civil Procedure (ZPO). Because of harmonisation of conflicts rules at the EU level in the form of *lois uniformes*, the relevance of German domestic conflict-of-laws rules in the EGBGB has been shrinking. Parts of the EGBGB have already been abolished.

The EGBGB is no comprehensive source of German domestic conflicts rules. For one, there are non-codified[37] conflicts rules, for example in the field of company law. For another, some acts for particular areas of substantive private law themselves contain conflicts provision(s) for the respective area of law. In the context of securities, one can point to Article 91 *et seq.* of the Bills of Exchange Act (*WechselG*) and Article 60 *et seq.* of the Checks Act (*ScheckG*) which are based on conventions.[38] They do not address, however, the transfer of the respective securities. There is also § 17a of the Securities Account Act. Not least, as § 32 of the e-Securities Act expressly refers to it, this decades-old provision has gained relevance for e-securities.[39]

The EGBGB itself does not contain conflicts provisions dealing with securities in particular. In fact, the German legislator consciously decided against introducing such rules when codifying the conflicts rules for rights *in rem*.[40] To the extent that the legal relationship documented in a security is affected by the rights *in rem* in the security, however, Article 43 of the EGBGB as the general conflicts provision for rights *in rem* will apply[41] (unless pre-empted by a special rule, of course). It sets forth the well-known and widely-used *situs* rule, using the location of a thing as the connecting factor. Article 46 of the EGBGB provides for an escape clause. The parties cannot choose the law applicable to rights *in rem* under German conflicts rules.

The EGBGB is the only place in German law where to find (albeit only a few) general rules, *i.e.* rules relevant for more than one – indeed, in several instances for every – special conflicts rules.[42] Apart from the declarative rule of Article 3 of the EGBGB on the sources of conflicts rules for Germany, the EGBGB addresses six general issues: Article 4(1) and (2) clause 1 of the EGBGB concerns *renvoi*, Article 4(2) clause 2 of the EGBGB addresses a detail in the context of

37 One hesitates to write "not yet," as in many fields, codification does not appear to be on the political agenda.

38 Namely the 1930 Geneva Convention about Provisions in the Area of Private International Law of Bills of Exchange (Imperial Law Gazette 1933 II, 377) and the 1931 Geneva Convention in the Area of Private International Law of Checks (Imperial Law Gazette 1933 II, 537, 595).

39 In more detail, *infra* sec. 2.2.3.

40 BT-Drs. 14/343, 1 February 1999, 14.

41 Spindler (n 33), 728; Wendehorst (n 32), para. 201; Mansel (n 32), paras. 24–26.

42 On this concept Wilke (n 36), 281–82 and passim.

party autonomy,[43] Article 4(3) of the EGBGB is about states with more than one legal system, Article 5 of the EGBGB pertains to issues of nationality and (habitual) residence as connecting factors, and Article 6 of the EGBGB contains the public policy reservation. It is to be assumed that these general provisions also apply to conflicts provisions located in acts other than the EGBGB. To be sure, statutory law is not entirely clear in this regard.[44] The EGBGB itself does not set forth that its general rules have relevance for other conflicts rules as well. One could interpret the heading "general provisions" above Article 3 of the EGBGB in this way, but the term "general" might also be limited to the other conflicts rules of the EGBGB itself. Special conflicts rules located in other acts generally do not expressly refer to Article 4 *et seq.* of the EGBGB either. Since the general rules of the EGBGB reflect the legislator's stance on certain issues for a variety of special conflicts rules at least within the EGBGB, however, it stands to reason that they should also apply to other special conflicts rules if these rules contain no exceptions. This seems particularly persuasive for the public policy clause, for it would be absurd to assume that the application of foreign private law as mandated by conflicts rules in special acts should not be subject to the boundaries of public policy. In accordance with these general observations, the relevance of Article 4 *et seq.* of the EGBGB for the e-Securities Act will be examined in the following where pertinent.

2.2.3 The Relationship between § 32 of the e-Securities Act and § 17a of the Securities Account Act

It should be noted that § 32 of the e-Securities Act is only to apply "to the extent that § 17a of the Securities Account Act does not apply." The relationship between the two provisions as such is clear-cut in the sense of "either/or." At the same time, the notoriously difficult and much-debated[45] interpretation

43 It concerns the question of whether parties, to the extent that they can choose the applicable law, can choose conflicts rules – and provides a negative answer. As suggested in the text, this issue conceptually is best understood as one of party autonomy, not one of *renvoi*: *id.*, 202.

44 In the context of securities, see the diverging views of, on one hand, Fabian Reuschle, "Grenzüberschreitender Effektengiroverkehr: Die Entwicklung des europäischen und internationalen Wertpapierkollisionsrechts" (2004) 68 Rabels Zeitschrift für ausländisches und internationales Privatrecht 687, 723; Reinhard Ege, *Das Kollisionsrecht der indirekt gehaltenen Wertpapiere* (Berlin: de Gruyter 2006), 126 (both for application), and, on the other hand, Michael Born, *Europäisches Kollisionsrecht des Effektengiros*: *Intermediatisierte Wertpapiere im Schnittfeld von Internationalem Sachen-, Schuld- und Insolvenzrecht* (Tübingen: Mohr Siebeck 2014), 289 (only application by analogy).

45 Even more than twenty years after the provision was drafted, one could read that the issue of its scope had not yet been sorted out: Christopher Kranz, "IPR-Fragen bei der

of § 17a of the Securities Account Act has now become an integral part of the interpretation of § 32 of the e-Securities Act. The former provision can be translated as follows:

> **§ 17a Dispositions about Securities**
> Dispositions about securities or parts of collectively held securities that are recorded with constitutive effect in a register or entered into an account, are governed by the law of the state under whose supervision the register is maintained in which the recording is made with constitutive effect directly in favour of the receiving person, or in which the main or branch office of the depositary is located that credits the receiving person.[46]

In order to determine the respective scope of the conflicts provisions, it is first necessary to consider § 17a of the Securities Account Act against the backdrop of Directives 98/26/EC (Finality Directive) and 2002/47/EC (Financial Collateral Arrangements Directive). While the transposition of Article 9(2) of the Finality Directive was the occasion for the creation of § 17a of the Securities Account Act, the latter was intended to have a much broader scope from the beginning[47] – so much so that the German legislator did not consider any modifications of German law necessary when the time came to transpose Article 9 of the Financial Collateral Arrangements Directive.[48] In view of this background and because of the relative independence of PIL from substantive law,[49] it was generally accepted that § 17a of the Securities Account Act was not limited to securities documented in a piece of paper,[50] even though the

---

Verpfändung von Mitgliedschaftsrechten" (2021) 41 Praxis des Internationalen Privat- und Verfahrensrechts 139, 142.

46 The official German version reads: "**§ 17a Verfügungen über Wertpapiere** Verfügungen über Wertpapiere oder Sammelbestandanteile, die mit rechtsbegründender Wirkung in ein Register eingetragen oder auf einem Konto verbucht werden, unterliegen dem Recht des Staates, unter dessen Aufsicht das Register geführt wird, in dem unmittelbar zugunsten des Verfügungsempfängers die rechtsbegründende Eintragung vorgenommen wird, oder in dem sich die kontoführende Haupt- oder Zweigstelle des Verwahrers befindet, die dem Verfügungsempfänger die rechtsbegründende Gutschrift erteilt." ((Gesetz über die Verwahrung und Anschaffung von Wertpapieren) ("Depotgesetz")).

47 BT-Drs. 14/1539, 7 September 1999, 16.

48 BT-Drs. 15/1853, 29 October 2003, 12.

49 In more detail *infra* sec. 2.2.4.

50 *E.g.*, Sabine Dittrich, "§ 17a," in Peter Scherer (ed), *Depotgesetz* (*DepotG*)*: Kommentar* (München: C.H. Beck 2012), para. 36.

substantive scope of the Act, in fact, used to be. Article 4 of the Act Introducing e-Securities has now extended this scope to e-securities within the meaning of the e-Securities Act by creating a new § 1(1) clause 3 of the Securities Account Act.

As of today, one of the main bones of contention is the requirement of the recording having constitutive effect. The German version of Article 9(2) of the Finality Directive seems to prescribe as much[51] whereas versions in other languages are a lot more ambiguous.[52] Since the recording of a security – at least until now – typically did not have a constitutive effect under German law, it seemed that, paradoxically, § 17a of the Securities Account Act could not encompass the vast majority of dispositions under German law.[53] This is one of the reasons why some authors have considered the scope of application of § 17a of the Securities Account Act to be rather slim (thus far).[54] For § 32 of the e-Securities Act, however, this conclusion could have resulted in a broad scope of application: the narrower the one, the broader the other.

Yet it is also rather obvious that § 17a of the Securities Account Act must apply to e-securities because of the very mentioning of this provision in § 32(1) of the e-Securities Act. Without the former being applicable to e-securities at all, there could not be any potential overlap with the latter in need of a solution. The extension of the substantive scope of the Securities Account Act also militates in favour of some relevance of the conflicts rule in the context of e-securities.

A relatively easy line between § 17a of the Securities Account Act and § 32 of the e-Securities Act can be drawn if one starts from the realisation that the Securities Account Act including its conflicts rule only pertains to securities in

51 "[M]it *rechtsbegründender Wirkung* in einem Register eingetragen" (emphasis added). § 17a Securities Account Act uses the exact same terminology in this regard (see n 44).

52 English: "legally recorded on a register." French: "est inscrit légalement dans un registre." Italian: "è legalmente registrato in un libro contabile." Spanish: "se inscriba legalmente en un registro." See Dorothee Einsele, "Die internationalprivatrechtlichen Regelungen der Finalitätsrichtlinie und ihre Umsetzung in der Europäischen Union" (2001) Wertpapier-Mitteilungen 2415, 2419; but also Matthias Lehmann, *Finanzinstrumente*: *Vom Wertpapier- und Sachenrecht zum Recht der unkörperlichen Vermögensgegenstände* (Tübingen: Mohr Siebeck 2009), 494.

53 Lehmann (n 52) (pointing out, however, that the terminology does make sense for dispositions under the law of other states); Reuschle (n 44), 720; Einsele (n 52), 2421; but also Ulrich Segna, *Bucheffekten*: *Ein rechtsvergleichender Beitrag zur Reform des deutschen Depotrechts* (Tübingen: Mohr Siebeck 2018), 381; Ege (n 44), 114.

54 Somewhat ironically, in the context of *electronic* securities in individual recording, recordings now actually do have constitutive effect (see in particular § 24 of the eWpG (n 9)).

collective custody.[55] Conversely, § 17a of the Securities Account Act does not apply to securities in individual custody. Emphasising the parallels between collective custody of securities and the collective recording of e-securities,[56] one would apply § 17a of the Securities Account Act to e-securities in collective recording.[57] It would follow that § 32 of the e-Securities Act only applies to e-securities in individual recording (again, typically in a crypto-securities register[58]).[59]

2.2.4 The Remaining Subject Matter of § 32 of the e-Securities Act

Having established that § 32 of the e-Securities Act concerns e-securities in individual recording, it is necessary to analyse in more detail which e-securities are specifically covered by the provision. Because of its position in the final chapter of the e-Securities Act, there can be little doubt that the conflicts rule covers both central register securities and crypto-securities.

The substantive limitation of § 1 of the e-Securities Act to bearer bonds is a bit more problematic. It could mean that § 32 of the e-Securities Act encompasses (German?)[60] bearer bonds only (whether in a register supervised by German authorities or by authorities of another state). But German PIL doctrine has long recognised that definitions for certain terms under substantive law do not (necessarily) limit the interpretation of the same terms if they appear in a conflicts rule. The conflicts rule would otherwise not be able to cover foreign phenomena even if they are functionally equivalent to a feature of domestic substantive law. This would not make much sense for an omnilateral conflicts rule. It would lead to gaps in PIL that somehow would have to be filled anyway in order to avoid denial of justice. In light of these considerations applicable to

55 Christian von Bar and Peter Mankowski, *Internationales Privatrecht II* (2nd edn, München: C.H. Beck 2019), § 3 para. 157; Wendehorst (n 32), para. 248; Mansel (n 32), para. 68; Dittrich (n 50), para. 62.

56 *Supra* sec. 2.1.2.

57 This is what Laurenz Wieneke and Jens H. Kunz, "Das Gesetz zur Einführung von elektronischen Wertpapieren: Der Regierungsentwurf" (2021) Neue Zeitschrift für Gesellschaftsrecht 316, 323 and Ulrich Segna, "Elektronische Wertpapiere im zentralen Register: Anmerkungen zum BMF-/BMJV-Referentenentwurf vom 10.8.2020 aus wertpapier- und depotrechtlicher Sicht" (2020) Wertpapier-Mitteilungen 2301, 2311, already suggested on the basis of (different versions of) the draft Act.

58 *Supra* sec. 2.1.2.

59 To this effect also Oliver L. Knöfel, "Elektronische Wertpapiere im Internationalen Privatrecht" in Helmut Grothe and Peter Mankowski (eds), *Festschrift Christian von Bar* (München: C.H. Beck 2022), 167.

60 Lehmann (n 31), "Zeitenwende im Wertpapierrecht: Der Referentenentwurf für ein Gesetz über elektronische Wertpapiere (eWpG)," 432 (with fn 12).

all (omnilateral) conflicts rules, it is generally recognised in Germany that characterisation must be carried out from a functional-teleological perspective.[61] This means in particular that limitations under substantive law do not have to restrict the understanding of a term used in a conflicts rule. Therefore, the meaning of e-securities under German substantive law and the limitation of the entire Act to bearer bonds should not be understood to necessarily restrict the subject matter of § 32 of the e-Securities Act.

Even so, the devil is in the details. For example, in light of the German legislator not wanting to make rules about electronic shares,[62] must § 1 of the e-Securities Act be interpreted to limit § 32 of the e-Securities Act at least categorically, *i.e.* to securities about obligations? And if so, could the resulting gap be closed by applying § 32 of the e-Securities Act, after all, only by analogy? As all connecting factors depend on the existence of a register, however, it at least seems reasonable to assume that the subject matter of § 32 of the e-Securities Act only covers foreign securities if they are recorded in a register. It is also obvious from the way the provision is phrased that it only concerns the law applicable to rights *regarding* the e-security, not rights *deriving from* the e-security.[63]

2.2.5 The Connecting Factors of § 32 of the e-Securities Act

§ 32(1) of the e-Securities Act designates a state's supervision over the e-securities register office in whose register the e-security at issue is recorded as the primary connecting factor. In this way, the determination of the applicable substantive private law is tied to a state's international supervisory competence: a preliminary[64] question of administrative international law. Rules for the competence of state authorities in the international dimension themselves use connecting factors. Thus, to make supervision by a state authority relevant for a rule of PIL is tantamount to making the respective connecting factors under administrative international law relevant for the determination of the applicable private law.

Connecting factors under administrative international law are likely to vary from state to state. Some states might condition their exercise of regulatory

61 See Abbo Junker, *Internationales Privatrecht* (5th edn, München: C.H. Beck 2022), § 7 para. 28 et seq.

62 *Supra* sec. 2.1.1.

63 As to the distinction, see *supra* sec. 2.2.1. For the reasonableness of distinguishing these two dimensions for electronic securities as well, see *e.g.*, Knöfel (n 59), 160 et seq.

64 As suggested elsewhere (Wilke (n 36), 121–24), the term "preliminary question" should be used to designate legal issues presupposed by a conflicts rule, as opposed to the "incidental question" which concerns (the determination of the applicable law to) a legal issue raised in the context of the applicable law.

authority on the seat of a person, others will focus on a person carrying out (certain parts of) their business within the state's territory. For Germany, for example, the Federal Administrative Court has interpreted the requirements of § 32(1) of the Banking Act[65] (carrying out banking business or financial services *domestically*) to mean that a bank must carry out at least parts of its business in Germany; these parts must consist in substantial steps towards the conclusion of a contract.[66] It follows that the same business activity can be subject to more than one state's supervision[67] or might not even be subject to supervision at all.[68] The first scenario might make compliance rather tricky, the second might be a dream come true for some businesses. From the PIL perspective, however, neither one is acceptable. There must be one applicable private law.

As far as the potential accumulation of applicable laws is concerned, one needs a tie-breaker: an additional rule to select the one applicable law. Conceptually speaking, this could even be a rule setting forth that a mix of the different laws should be applied.[69] Neither § 32 of the e-Securities Act nor any other provision of German law, however, contains a pertinent

65 There is no provision of German law expressly setting forth its international supervisory competence with regard to e-securities registers. § 11 of the e-Securities Act (eWpG (n 9)) (*supra* sec. 2.1.1) only concerns the substantive scope of the Federal Financial Supervisory Authority. It is impossible to derive an answer from it to the issue of international competence, as it contains nothing even similar to a connecting factor. § 32 of the Banking Act (n 17) then seems to be the best choice as it requires certain businesses to obtain authorization from the Federal Financial Supervisory Authority. This implies the latter's international competence. Yet it is even more complicated than that, as the maintenance of a *central* register does not require authorization under § 32 of the Banking Act (n 17). As such, this makes sense, because only central securities depositories and depositary banks can maintain this type of register (*supra* sec. 2.1.2), and these types of businesses need authorization for their activities, anyway. But for the purposes of § 32 e-Securities Act (eWpG (n 9)), one probably must apply § 32 of the Banking Act (n 17) by analogy. In more detail see Michael Müller, "§ 32," in Michael Müller and Christian Pieper (eds), *Gesetz über Elektronische Wertpapiere* (München: C.H. Beck 2022), paras. 18–20.

66 BVerwG, Judgment of 22 April 2009 – 8 C 2/09, (2009) Wertpapier-Mitteilungen 1553, para. 36.

67 State A might use the seat of company C in its territory as the relevant connecting factor and thus supervise C's activities, whereas State B might use C's activities in its territory as the relevant connecting factor and thus also supervise C's activities.

68 If we switch the relevant connecting factors in the preceding example (n 67), State A might not supervise C because C has no relevant activities in A's territory (only in B), and State B might not supervise C, either, because C's seat is in A.

69 Such an approach is not unheard of in EU private international law; see in particular Art. 6(2) cl. 2 Rome I Regulation (Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), [2008] OJ L177/6) ("Rome I").

tie-breaker.[70] Yet there must be a solution, the determination of no applicable law at all meaning a denial of justice. A functionally equivalent rule is Article 5(1) of the EGBGB on multiple nationalities. There, as here, a connecting factor under PIL has become ambiguous because of a reference to public law, and now a solution for the purposes of PIL must be found. Under Article 5(1) clause 1 of the EGBGB, the state (of all the states whose nationality a person has) with which the person has the closest connection will be relevant. But if one of the nationalities is that of Germany, it will be decisive even if the person is not most closely connected to Germany (Art. 5(1) cl. 2 EGBGB).

In the absence of any apparent better solution, one can apply Article 5(1) of the EGBGB by analogy to determine the applicable law in cases of more than one state with supervisory authority.[71] Accordingly, if Germany has international supervisory competence over a given e-securities register, § 32(1) of the e-Securities Act would always lead to German law. This would have the practical advantage that it would not be necessary to analyse any other country's laws once Germany's competence has been established. Only in cases where Germany has no supervisory competence, one would even need the further step of taking into account foreign law. Of more than one relevant law, the one would be applicable to which the register office is most closely connected.

The second scenario – no applicable law under § 32(1) of the e-Securities Act because of no state imposing its supervision – is much easier to resolve. § 32(2) of the e-Securities Act provides subordinate connecting factors. The German legislator seems to have noticed at the last second that the connecting factor of state supervision of e-securities register can fail.[72]

Pursuant to § 32(2) clause 1 of the e-Securities Act, the seat of the respective register office is decisive if it is not under supervision. It is submitted that "supervision" means "state supervision" (as in paragraph 1). Otherwise, the provision could not catch all cases that are not subject to paragraph 1, and there still could be gaps, for example where a supranational institution like the ECB exercises supervisory functions. If the seat of the register office cannot be determined, § 32(2) clause 2 of the e-Securities Act connects the case to the law of the seat of the issuer. With regard to legal persons, "seat" must be

70 For a different view see Knöfel (n 59), 169 et seq.: Application of § 32(2) e-Securities Act. He reads the phrase "not under supervision" in § 32(2) e-Securities Act as "not under the supervision of just one state."

71 Müller (n 65), para. 32.

72 The Government Draft (n 12) only contained the connecting factor now found in paragraph 1. The Finance Committee of the German Federal Parliament introduced the second paragraph shortly before the Act was passed, Recommended Resolution and Report, BT-Drs. 19/29372, 5 May 2021, 61.

understood as the statutory seat.[73] To the extent that the provision applies to natural persons, the German word for "seat" (*Sitz*) seems to suggest the relevance of a person's domicile (*Wohn*sitz), yet it seems more plausible to interpret it as meaning a person's habitual residence.[74]

2.2.6 The Governing Law as Determined by § 32 of the e-Securities Act

At the outset, it should be noted that § 32 of the e-Securities Act is an omnilateral[75] conflicts provision. It is capable of determining as applicable any (state) law in the world. If the application of foreign law resulted in an obvious violation of German public policy (*ordre public*), German courts could pull the universally known ripcord. Under Germany's public policy reservation of Article 6 clause 1 of the EGBGB, the foreign law would not be applied. In such a scenario, German courts would ultimately resort to the application of German law to the extent that a modified application of foreign law is not possible.[76]

§ 32 of the e-Securities Act does not address whether it refers to another state's substantive law or PIL rules. In particular, it does not refer to "substantive provisions" which under Article 4(2) clause 1 of the EGBGB would – obviously – be considered an exclusion of *renvoi*. One thus has to resort to the general provision, *i.e.* Article 4(1) clause 1 of the EGBGB, pursuant to which a reference to foreign law is "also" a reference to its PIL rules unless this runs afoul of the purpose of the respective reference. The "also," of course, is simply poor phrasing, albeit not exclusive to German PIL.[77]

Scholars almost unanimously hold that § 17a of the Securities Account Act, due to its origin in EU directives, does not allow *renvoi*.[78] That provision and § 32 of the e-Securities Act being counterparts in the context of *electronic* securities, one might conclude that there should also be no *renvoi* in the context of the latter. On the other hand, § 32 of the e-Securities Act complements Article 43(1) of the EGBGB in that the one covers electronic *securities*, while the other covers *securities* documented in a piece of paper. Prevailing opinion has it that Article 43(1) of the EGBGB allows *renvoi*.[79] This militates in favour of § 32 of the

73 Wilke (n 8), 507; Müller (n 65), para. 31.

74 Wilke (n 8), 507; Müller (n 65), para. 31.

75 Most would probably prefer the term "multilateral." For the not-just-theoretical distinction between "unilateral," "multilateral," and "omnilateral," however, see Wilke (n 36), 4.

76 BGH, Judgment of 11 October 2006 – XII ZR 79/04, (2007) Neue Juristische Wochenschrift Rechtsprechungs-Report Zivilrecht, 149.

77 Wilke (n 36), 249 with further references.

78 Dittrich (n 50), para. 70 et seq; Born (n 44), 289; Ege (n 44). It seems that only Reuschle (n 44) has suggested to assume an exclusion of *renvoi* solely for those parts of the § 17a Securities Account Act that are based on EU law.

79 Junker (n 61), § 17 para. 3; Wendehorst (n 32), para. 117; Mansel (n 32), para. 1146.

e-Securities Act allowing *renvoi* as well. Since the basic stance of German PIL is the admission of *renvoi* and, in light of the foregoing conclusions, as it is not obvious that this would run afoul of § 32 of the e-Securities Act, this second approach is to be preferred.[80]

Where the first paragraph of § 32 of the e-Securities Act refers to a state with more than one legal system, the last step in the determination of the applicable law is left to that state's internal conflicts rules, Article 4(3) clause 1 of the EGBGB. In the absence of pertinent rules, the law with which the case is most closely connected applies pursuant to Article 4(3) clause 2 of the EGBGB. The analysis is different for the second paragraph. Since both connecting factors in § 32(2) of the e-Securities Act are a person's (either the register office's or the issuer's) seat,[81] German PIL itself already sets forth which legal system is relevant. It would be unnecessary to apply the rule of Article 4(3) of the EGBGB. In fact, the said provision expressly requires that the relevant legal system has not yet been indicated, and thus would not apply.

3. Blockchain in German PIL in General

As mentioned at the very beginning, German law does not yet deal with blockchain in particular, which also means that there are no special conflicts rules for blockchain. Yet this does not release a judge from the duty to determine the applicable law in a case that, in some way, involves a blockchain – nor can or should lawyers (and/or the parties themselves)[82] involved in a transaction simply ignore the issue of the applicable law just because the transaction is connected to a blockchain. Rather, the effect of existing German (EU) conflicts rules must be analysed (*infra* 3.1). As regards potential legislative developments, one might wonder whether the German legislator should extend the solution of § 32 of the e-Securities Act to other blockchain contexts (*infra* 3.2) or whether different solutions suggest themselves (*infra* 3.3).

80 Accord Knöfel (n 59), 169.

81 *Supra* sec. 2.2.5.

82 To paraphrase a practitioner's perspective (Peter Scherer, *Blockchain im Wertpapierbereich* (Tübingen: Mohr Siebeck 2020), 137): those who are enthusiastic about a new technology and consider the "old" law as well as the bodies for enforcing it, irrelevant, are typically among the first who want to enforce a (presumed) legal position of theirs, including going to court, if something goes wrong.

3.1 *Other Relevant Conflicts Rules/Connecting Factors*

The determination of the law applicable to a contractual obligation typically is not influenced by the parties making use of blockchain technology. Thus, the respective conflicts rules already in force remain relevant even if blockchain plays a part in the implementation/execution of the contractual agreement, for example, in the form of so-called "smart contracts."[83] The same is true for obligations concerning digital assets.[84] For Germany, this by and large means the application of the conflicts provisions found in Rome I,[85] supplemented, where necessary, by German conflicts provisions (*e.g.* for questions of capacity because of Article 1(2)(a) of Rome I). If, for example, the parties have agreed to use blockchain technology in the context of the supply chain, the blockchain is part of the parties' performance of their contractual duties, which is governed by the law applicable to the contract determined by Article 3 *et seq.* of Rome I (see Art. 12(1)(b) of Rome I).[86] The relevant conflicts rules may include the special rules for consumer and individual employment contracts (Art. 6 and 8 of Rome I). The main connecting factors are a choice of law by the parties[87] and the habitual residence of one of the parties to the respective contract. As a consequence, different contractual relationships (*e.g.* along a global supply chain) relying on one and the same blockchain can be subject to different applicable laws. Yet this will usually correspond to the parties' expectations.[88] The same considerations – determination of the applicable law depending on the type of contract – apply for smart contracts.[89]

---

83 Georgina Garriga Suau, "Blockchain-based smart contracts and conflict rules for business-to-business operations" (2021) Revista Electrónica de Estudios Internacionales 21; Gerald Spindler, "Blockchain-Transaktionen und Vertrauensschutz," in Uwe Blaurock and Felix Maultzsch (eds), *Vertrauensschutz im Digitalen Zeitalter* (Baden-Baden: Nomos 2020), 56; Giesela Rühl, "Kapitel 12, Smart Contracts und anwendbares Recht," in Tom Braegelmann and Markus Kaulartz (eds), *Rechtshandbuch Smart Contracts* (München: C.H. Beck 2019), para. 11.

84 Christiane Wendehorst, "Digitalgüter im Internationalen Privatrecht" (2020) 40 Praxis des Internationalen Privat- und Verfahrensrechts 490.

85 Rome I Regulation (n 69).

86 Anton S. Zimmermann, "Blockchain-Netzwerke und Internationales Privatrecht – oder: der Sitz dezentraler Rechtsverhältnisse" (2018) 38 Praxis des Internationalen Privat- und Verfahrensrechts 566, 568.

87 As to party autonomy conceptually being an issue of the connecting factor, see (with further references) Wilke (n 36), 197–98.

88 Zimmermann (n 86).

89 Spindler (n 83); Dieter Martiny, "Virtuelle Währungen, insbesondere Bitcoins, im Internationalen Privat- und Zivilverfahrensrecht" (2018) 38 Praxis des Internationalen Privat- und Verfahrensrechts 553, 559–60.

For non-contractual obligations in the blockchain context, the relevant conflicts rules for Germany will typically be those of Rome II.[90,91] The pertinent connecting factors under Rome II are a choice of law by the parties (Art. 14 of Rome II – in many cases only of theoretical interest[92]), the common habitual residence of the tortfeasor and the person sustaining damage (Art. 4(2) of Rome II) and the place where the damage occurs (Art. 4(1) of Rome II). The connection to an existing or hypothetical (contractual) relationship is also relevant both for torts and other non-contractual obligations (Art. 4(3), 10(1), 11(1), 12(1) of Rome II).

The relationship between the different participants in a given blockchain is more difficult to assess from the perspective of German PIL. Due to the element of cooperation, one might think of company law.[93] The first (minor) obstacle then is that Germany has not codified its conflicts rules for companies. Rather, this is an area where court decisions serve as the relevant source of law.[94] Germany's main approach still is the theory of the real seat, *i.e.* the application of the law of the place where a company/partnership has its principal place of administration.[95] In cases of companies founded in another EU/EEC Member State, however, German courts will apply the law of the respective company's statutory seat (registered office)[96] in line with the rich case law of the European Court of Justice[97] concerning the freedom of establishment of companies and firms (Art. 54, 49 TFEU).[98] The second (major) obstacle results from this dual approach: both connecting factors do not work for many

90 Regulation (EC) No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II), [2007] OJ L199/40 ("Rome II").

91 Martiny (n 89), 564.

92 Also Tobias Lutzi, "The Tort Law Applicable to the Protection of Crypto Assets," in this volume, sec. 6 (414).

93 Law concerning associations, whether incorporated or not. Also see Jonas Drogemüller, *Blockchain-Netzwerke und Kryptotoken im IPR* (Baden-Baden: Nomos, 2023), 102 et seq.

94 *Supra* sec. 2.2.2.

95 See only BGH, Judgment of 27 October 2008 – II ZR 158/06, Neue Juristische Wochenschrift, 2009, 290.

96 See only BGH, Judgment of 13 March 2003 – VII ZR 370/98, Neue Juristische Wochenschrift, 2003, 1461.

97 In particular: CJEU, Judgment of 9 March 1999 – *Centros Ltd v. Erhvervs- og Selskabsstyrelsen* (C-212–97), Neue Juristische Wochenschrift, 1999, 202; CJEU, Judgment of 5 November 2002 – *Überseering BV v. Nordic Construction Company Baumanagement GmbH* (C-208/00), Neue Juristische Wochenschrift, 2002, 3614; CJEU, Judgment of 30 September 2003 – *Kamer van Koophandel en Fabrieken voor Amsterdam v. Inspire Art Ltd* (C-167/01), Neue Juristische Wochenschrift, 2003, 3331.

98 Other treaties can mandate the application of the law of the company's statutory seat, as well. In particular, this concerns companies with their statutory seat in the USA because

blockchains; there typically is no incorporation in any State nor is it often possible to determine a principal place of business.[99] This might be an indication that company law is simply the wrong legal category to think about (these) blockchains in the first place.[100] One then would probably characterise the relationship as contractual for the purposes of PIL[101] – which, of course, does not mean that the substantive law applicable pursuant to Rome I will consider a contract to even have come into existence.[102] In particular regarding cooperation agreements in decentralised (autonomous) organisations, however, the two connecting factors of company law might have to be replaced by the location of the deciding court for lack of a better solution. In other words, one would apply the *lex fori*.[103]

Finally, the determination of the correct conflicts rule for (potential) rights with third party effects in digital assets on a blockchain proves tricky. At least for permissionless blockchains, the location of the asset in question would be impossible to establish – yet this is exactly what Article 43(1) of the EGBGB mandates.[104] It has been suggested to rely on the escape clause of Article 46 of the EGBGB and look for the closest connection.[105] The conceptual problem with this approach is that escape clauses generally require that an applicable law *has been* determined on the basis of another conflicts rule, but that this applicable law is (substantially) less connected to the case than another.[106] The wording of Article 46 of the EGBGB itself is quite clear in this regard.[107] Rather, one would need a subsidiary conflicts rule for this situation. But Germany's written conflicts provisions for rights *in rem* do not contain such a rule.

---

of Art. XXV(5) of the 1954 Treaty of Friendship, Commerce and Navigation between the United States of America and the Federal Republic of Germany, No. 3943.

99 Gerald Spindler, "Blockchaintypen und ihre gesellschaftsrechtliche Einordnung: Unter besonderer Berücksichtigung der *decentralized autonomous organization* (DAO)" (2021) Recht Digital 314 (also regarding exceptions); Zimmermann (n 86), 568 (and 570); also Maximilian Mann, "Die Decentralized Autonomous Organization – ein neuer Gesellschaftstyp?" (2017) 20 Neue Zeitschrift für Gesellschaftsrecht 1014, 1018–19.

100 Zimmermann (n 86); also Drogemüller (n 93), 110 et seq.

101 Dariusz Szostek, *Blockchain and the Law* (Baden-Baden: Nomos 2019), 72–77.

102 Andrew Dickinson, "Cryptocurrencies and the conflict of laws," in David Fox and Sarah Green (eds), *Cryptocurrencies in Public and Private Law* (Oxford: Oxford University Press 2019), para. 5.31 (and paras. 5.35 et. Seq. for an in-depth analysis of the different conflicts rules).

103 In more detail Spindler (n 99), 314–15; Zimmermann (n 86), 570–71.

104 *Supra* sec. 2.2.2.

105 Wendehorst (n 84), 496.

106 Wilke (n 36), 183–87.

107 "[S]ubstantially closer connection to a law other than the one that would be relevant pursuant to Articles 43 and 45."

Accordingly, in line with the idea expressed in Article 46 of the EGBGB, it ultimately does seem most appropriate to rely on the idea of the closest connection. This connection will depend on the individual circumstances of the case.[108] If all else fails, a court should probably apply the *lex fori* notwithstanding the disadvantages of such a solution.[109]

3.2 *The e-Securities Act as a Model?*

As demonstrated above, the e-Securities Act as such is limited to one particular type of securities, *i.e.* bearer bonds,[110] and § 32 of the e-Securities Act, albeit undoubtedly of a broader scope, (likely) is not all-encompassing.[111] This invites the question of whether § 32 of the e-Securities Act can serve as a model for further legislation. To be sure, the draft Act first expressly stated that the Act should not be understood as precedent for other areas.[112] But parts of the instrument were deliberately phrased in such a way as to accommodate potential extensions at a later stage.[113] It is thus quite clear that the legislator was aware that the Act is likely to have some influence on future legislative developments. It is equally obvious that the legislator did not specifically think about the conflicts rule in this context. The same considerations apply, however. Thus, in the following, it will be analysed whether § 32 of the e-Securities Act can serve as a model for other blockchain-related conflicts rules. In particular, this means looking at the suitability of its connecting factors for other fields; its subject matter would change, naturally. Yet some aspects of the drafting of § 32 of the e-Securities Act as regards subject matter and governing law will be factored in as well.

3.2.1 Advantages

One main advantage of using state supervision as the connecting factor (as in § 32(1) of the e-Securities Act) is the alignment of regulatory and (substantive) private law. A business and its transactions are subject to regulatory duties of (at least: also)[114] the state whose law applies to the private law effects of said transactions. The people running the business will only have to acquaint

108 See the analysis by Wendehorst (n 84), 496–98.
109 Spindler (n 33), 736–37.
110 *Supra* sec. 2.1.1.
111 *Supra* sec. 2.2.4.
112 Government Draft (n 12), 30.
113 See *id.*, 49, explaining why terminology broader than would be necessary only for bearer bonds is used in this instance.
114 It is possible that more than one state assumes international supervisory competence, *supra* sec. 2.2.5.

themselves with and seek advice for one legal system. In practice, it would not even be necessary to make a distinction between regulatory and private law because the relevant rules would be found in one and the same legal system anyway. Where regulatory and private law questions are interwoven, for example where a claim for damages is based on non-compliance with banking law,[115] a court seized in the respective state can likewise (relatively) simply apply its own law to all questions.

Where the use of blockchains is subject to regulatory requirements, lawmakers have identified "regulatory access points."[116] The law then already imposes legal obligations on one or more persons in some way connected to blockchains in spite of their decentralised nature. The specific measures typically depend on the type of blockchain and the purpose for which it is used. It is much easier to identify (potential) subjects for legal obligations in a permissioned blockchain than in a permissionless blockchain.[117] In light of the foregoing observations, state supervision turns out to be a reasonable connecting factor for certain fields. Because of the public interests at stake, many states have, in these fields, already established or are likely to establish regulatory requirements, the implementation of which they (will) monitor. At the same time, this approach overcomes the problem of not being able to pinpoint the location of a thing (like a paper security) as more traditional conflicts rules might require. A provision like § 32(1) of the e-Securities Act could therefore relatively easily be employed in other areas with a certain (minimum) degree of regulation. (Implicit in this statement are the limitations of state supervision as the main connecting factor to be explained momentarily.)[118]

In principle, the existence of subordinate connecting factors can also be regarded as an aspect of § 32 of the e-Securities Act worthy of replication. The people charged with applying the law – whether the parties/lawyers long before any dispute or a court in case of litigation – should not be left high and dry if it can be foreseen that a certain connecting factor might not work in all

115 See Matthias Lehmann, "§ 1 Das Finanzmarktrecht im Internationalen Privatrecht," in Dirk Zetzsche and Matthias Lehmann (eds), *Grenzüberschreitende Finanzdienstleistungen: Das internationale Finanzmarkt-, Privat- und Zivilprozessrecht Deutschlands, Österreichs, der Schweiz und Liechtensteins* (Tübingen: Mohr Siebeck 2018), para. 7.

116 In more detail Finck (n 24), 45–58.

117 In much more detail, Andreas Kerkemeyer, "Herausforderungen des Blockchain-Netzwerks für das Kapitalmarktrecht" (2020) 49 Zeitschrift für Unternehmens- und Gesellschaftsrecht 654, 674–85; also Eduard Hofert, *Regulierung der Blockchains*: *Hoheitliche Steuerung der Netzwerke im Zahlungskontext* (Tübingen: Mohr Siebeck 2018), 229–30 (and passim); Finck (n 24), 195.

118 *Infra* sec. 3.2.2.

cases. If one were to transfer the conflicts provision to other fields with less regulation, additional connecting factors would be even more important.[119] In particular, the seat of the issuer (§ 32(2) cl. 2 e-Securities Act) is a reasonable connecting factor in and of itself (corresponding to the idea of "LIMA": Location of the Issuer Master Account) and could be used in other contexts as well.[120]

A further advantage of a rule like § 32 of the e-Securities Act is its technological neutrality. It is not contingent on the existence of a blockchain.[121] It applies to other types of electronic registers as well. The transfer of such a rule to a different field in which blockchain is only one of more relevant technologies is relatively easy. This corresponds to the idea expounded in the preceding section that the special features of blockchains do not always constitute the relevant characteristics of a case for the purposes of PIL.

Finally, although the statement might seem redundant in the 21st century, the omnilateral nature of § 32 of the e-Securities Act should be considered a positive aspect. To provide only for the application of one's own law would be short-sighted, not least in the blockchain context.

3.2.2 Disadvantages

The first drawback of § 32(1) of the e-Securities Act lies in its vague reservation to another rule, *i.e.* to § 17a of the Securities Account Act. This particular way of phrasing the conflicts rule leads to all sorts of problems surrounding the correct understanding of § 32 of the Securities Act.[122] At the same time, this is an issue not likely to reappear in a future conflicts rule for other blockchain questions. The reference to § 17a of the Securities Account Act is due to the particularities of (electronic) securities, after all.

More problematic as a general matter is the choice of the connecting factor in § 32(1) e-Securities Act. To be sure, as a matter of legislative technique, there is nothing inherently wrong with making connecting factors used in administrative international law relevant for PIL. For somebody charged with determining the applicable private law, however, this has some unattractive consequences.

First, it means the (theoretical)[123] necessity to analyse the law of all states that might possibly want to exercise their regulatory authority in the given

119 But one would often have to question the legislator's overall approach, *infra* sec. 3.2.2.

120 Wendehorst (n 84), 497; Spindler (n 33), 732.

121 *Supra* sec. 2.1.3.

122 *Supra* sec. 2.2.3.

123 First, not all practitioners might want to carry out this task. Secondly, if one follows the approach suggested here (*supra* sec. 2.2.5), it would often be sufficient to determine that Germany has supervisory competence.

case. Not only can this amount to a lot of work, it can also be a lot of difficult work:[124] to ascertain and apply foreign law is no easy task to begin with, and it is doubtful whether the field of (the international competence for the supervision of) financial regulation will make life particularly easy for the people concerned. To be sure, to ascertain foreign law as such is hardly an extraordinary occurrence in the realm of PIL.[125] But there is a difference between having to ascertain (and then apply) one private law and having to analyse the (public) law of potentially many states in order to even be able to decide which private law is applicable.

Second, it has already been demonstrated that this legislative technique can lead to more than one applicable law – or none at all. This, in turn, leads to further complex issues.[126] In an ideal world, the legislator would provide for special rules dealing with these issues. This has happened in part with § 32(2) of the e-Securities Act, but doubts remain for the situations not covered by this provision (and potentially also with regard to its scope in the first place).

On a more fundamental level, it is far from evident that the connecting factor of state supervision is the most adequate one for other areas in the blockchain context. It can potentially cause an undesired *conflit mobile*.[127] What is more, if there is no supervision by a state over the activity at issue, a rule designed like § 32(1) of the e-Securities Act simply fails, necessitating one or more subordinate connecting factors. Again, this raises no conceptual problem. Additional rules can be drafted (if the legislator notices the issue). As shown, this did happen with regard to § 32 of the e-Securities Act. But, for one, a subordinate connecting factor of the seat of the register office (§ 32(2) cl. 1 e-Securities Act) may itself not prove particularly suitable in the blockchain context where, as a matter of technology, no such "office" necessarily has to exist.[128] It is unlikely that governments will require the establishment of such offices for any and all blockchains. For another, it would not be very convincing to introduce a provision with state supervision as the main connecting factor to areas of law where there is no supervision in general (or at least not in most states). Not only would it be poor legislative technique to have a main rule that

124 For a more optimistic account see Knöfel (n 59), 168.

125 In this sense, in the context of international administrative/supervisory law, see also Lehmann (n 115), para. 17.

126 *Supra* sec. 2.2.5.

127 Robert Freitag, "§ 14 Internationales Privatrecht," in Florian Möslein and Sebastian Omlor (eds), *Tech-Handbuch* (München: C.H. Beck 2021), para. 37. On the *conflit mobile* in general, see *e.g.*, Wilke (n 36), 187–94.

128 Similarly, Freitag (n 127).

rarely, if at all, applies. But, and in particular, the suitability of a connecting factor is drawn into serious doubt if it typically does not exist.

Finally, another problem of § 32 of the e-Securities Act has proved to be its unclear stance on *renvoi*. In absence of an express indication, one can always point to Article 4(1) of the EGBGB and assign the onus of arguing against the admission of *renvoi* to those who wish to deviate from the basic rule. But then the legislator should at least expressly refer to provisions of substantive law (Art. 4(2) cl. 1 EGBGB) where it wants *renvoi* to be excluded.

3.3 *Other Approaches (?)*

As demonstrated above, where Rome I and Rome II are applicable in the blockchain context, one main connecting factor is the habitual residence of a person. This seems reasonable where blockchain technology is used for the implementation of a contractual agreement between parties (in some way) known to each other. In a transaction between parties remaining anonymous/pseudonymous or where a person who conceals his or her identity commits a tort, determination of habitual residence can raise serious practical difficulties. Similar problems with the "locational exercises"[129] required by PIL can arise, for example, regarding the determination of the place where a damage occurs.[130] But they do not automatically arise just because a tort case has some connection to a blockchain.[131] Not all of these issues are only germane to blockchains and/or entirely unprecedented. It is therefore doubtful that the holy grail of a perfect (new) solution can be found in the blockchain context specifically.

It has been suggested, albeit not with a particular focus on Germany, to apply the rules that are defined by consensus of the participants in a blockchain (*lex cryptographia*) and to set up special private dispute resolution mechanisms.[132] This is not the place to open the can of worms that is the discussion about the application of non-state law.[133] Suffice it to say that it can hardly be a panacea. Some degree of "interaction" between blockchain transactions and (legal rules

129 Matthias Lehmann, "Who Owns Bitcoin? Private Law Facing the Blockchain" (2019) 21 Minnesota Journal of Law, Science & Technology 93, 114.

130 See Lutzi (n 92), sec. 3.2 (408 et seq.).

131 *Id.*, 2.1 (400 et seq.); Dickinson (n 102), paras. 5.11–5.12.

132 Florence Guillaume, "Aspects of private international law related to blockchain transactions," in Daniel Kraus, Thierry Obrist and Olivier Hari (eds), *Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law* (Cheltenham: Edward Elgar 2019), 71–75. For the related notion of "blockchains as a regulatory technology," see also Finck (n 24), 66–87. Also see the examples for governance on a blockchain provided by Usha R. Rodrigues, "Law and the Blockchain" (2018) 104 Iowa Law Review 679, 717–21.

133 See some remarks by Lutzi (n 92), sec. 7 (414 et seq.).

in) the real world cannot be gainsaid.[134] For example, one would still require state (conflicts) rules for torts with a blockchain connection committed by people who are not participants in the respective blockchain. Furthermore, the potential for at least some degree of global uniformity of decisions appears at present even lower with this proposal than with the use of generally well-known connecting factors, even if not every state in the world uses the same one(s) and if some of them cause practical difficulties. For Germany in particular, I do not see the idea of non-state law for blockchains gaining much traction any time soon.

That said, one can certainly imagine taking more account of a consensus between the parties by allowing party autonomy.[135] This does not necessarily suggest itself as a general solution, however – at least not in an unfettered version. For one, this would threaten the synchronisation of regulatory and private law. Whether the resulting complexities[136] should be accepted/tolerated, depends on the respective field. For another, in particular where *in rem* effects are at issue, legitimate interests of third parties must be protected. From this perspective, choice of law should only be allowed in situations with a low number of participants.[137] Third, both a choice of law by the parties to the different transactions recorded on one blockchain and a "central" choice for all future transactions do not really match core tenets of blockchain philosophy (as far as permissionless blockchains are concerned[138]).[139] It is not clear whether the German legislator even considered the inclusion of party autonomy when drafting the e-Securities Act. The *travaux préparatoires* contain no indication to this effect.

4 Conclusion

As the silver bullet of an international, ideally global consensus[140] on the best approach for conflicts rules concerning blockchains does not (yet?) exist,

134 Guillaume (n 132), 75 admits as much. Also, Finck (n 24), 84–87.

135 *E.g.*, Scherer (n 82), 171–72; Spindler (n 83), 58; Guillaume (n 132), 78–79; Wendehorst (n 84), 497.

136 See *e.g.*, Lehmann (n 59), paras. 97–98.

137 See also Spindler (n 33), 734.

138 See Finck (n 24), 189–90 for an example of how hard it can be to reach consensus in a blockchain community even with regard to technological questions.

139 Lehmann (n 129), 112–14; against the idea of blockchain somehow being independent of courts and law, being immune to regulation, *e.g.*, Finck (n 24), 34–65.

140 For this desideratum *e.g.*, Wendehorst (n 84), 490; from the regulatory perspective *e.g.*, Finck (n 24), 59–60; from the substantive (uniform) law perspective Lehmann (n 129), 116.

solutions under national law must be considered. This chapter has examined the German perspective. There is no dedicated German conflicts rule for blockchains. It is neither likely nor desirable that a single such one-size-fits-all rule should be introduced. Blockchains can be used in different settings for different purposes – the most suitable conflicts provision (including, most importantly, the most suitable connecting factor) must be found for each one.[141] While the decentralised nature of blockchains with the random involvement of nodes causes huge problems in situations where PIL requires a focus on these features,[142] it has been demonstrated that not every connection of a case to a blockchain necessarily implies the latter's relevance for the determination of the applicable law.

It does make sense to design conflicts rules with a view to existing regulatory measures. This includes employing state supervision as the (main) connecting factor as the new § 32(1) of the e-Securities Act does. Similar provisions could be created for other fields with a certain (minimum) degree of regulation, in particular for financial services and the capital market.[143] One should make the caveat that the provisions should be drafted in a way that reduces the complexities, problems and drawbacks of § 32(1) of the e-Securities Act,[144] for instance by having the necessary supplemental rules in place for situations in which the rule refers to more than one state. To make the seat of the issuer of a financial instrument the relevant connecting factor (as a subordinate rule in § 32(2) clause 2 of the e-Securities Act) likewise is a reasonable approach. To the extent that a state uses the seat of the issuer as the basis for its international supervisory competence, the results would be the same (albeit probably easier to reach) as with state supervision as the connecting factor.

It would not be very persuasive, however, to consider § 32 of the e-Securities Act as a blueprint for all areas of (German) law in which blockchains (could) matter. First, the applicable law can be determined in many cases on the basis of existing (EU) conflicts rules. They have not proved to be so inadequate for blockchain-related scenarios as to need a general overhaul. Second, even where there is need for reform and/or entirely new rules, state supervision should only figure as a connecting factor if there typically is state supervision.

---

141 Similarly for regulatory measures Hofert (n 117), 60–61 (and passim); Spindler (n 83), 59.

142 Guillaume (n 132), 70; Lehmann (n 129), 112; Szostek (n 101), 76–77: with a focus on securities, Hubert de Vauplane, "Blockchain and intermediated securities" (2018) 1 Nederlands Internationaal Privaatrecht 94, 102; Spindler (n 33), 731.

143 See *e.g.*, Hofert (n 117).

144 *Supra* sec. 2.2.5 and *supra* sec. 3.2.2.

CHAPTER 25

DLT and PIL from the Perspective of Liechtenstein

Francesco A. Schurr and Angelika Layr

1 Introduction

As is generally known, blockchain and Distributed Ledger Technology (DLT) are (fairly new) technologies that come in different forms and shapes; from cryptocurrencies, tokenised securities to possible application for transparency and supply chain monitoring to personal identity security.[1] The large number of use cases has led to rising interest in the scientific community. Blockchain has been examined from a wide variety of perspectives and fields and has increasingly found its way into the legal debate. Some jurisdictions – like Liechtenstein – have already developed specific legislation to provide legal certainty for the emerging "Token Economy",[2] others – like Switzerland, Germany or France – have made selective legal adaptations.

Some crypto enthusiasts might follow the spirit of "code is law" and may not intend digital transactions to be governed by any law at all. Nevertheless, when it comes to judicial proceedings, the court will have to determine the law applicable to the specific case. Due to the non-uniform characterisation of crypto assets and digital transactions in different legal systems, there are uncertainties regarding the legal consequences. Therefore, it is of utmost interest to the market participants to achieve the applicability of the law of a jurisdiction that recognises the intended legal effects of token transactions.

It is the role of Private International Law (PIL) to determine the applicable law. The intangible and decentralised nature of blockchain-based crypto assets hinders the search for connecting factors within the categories of conflicts of laws. In this chapter, we outline Liechtenstein's path towards the so-called "Token Economy" and its approach to the conflict-of-laws challenges in this regard.

1 This paper was written in the context of a research project on DLT in Liechtenstein Private Law, financially supported by the Government of the Principality of Liechtenstein. The authors would like to thank the Government of Liechtenstein for the generous research-funding.

2 Thomas G. Dünser, *Legalize Blockchain! How States should deal with today's most promising Technology to foster Prosperity* (Norderstedt: BoD – Books on Demand 2020), 38–72.

© FRANCESCO A. SCHURR AND ANGELIKA LAYR, 2023 | DOI:10.1163/9789004514850_027
This is an open access chapter distributed under the terms of the CC BY-NC-ND 4.0 license.

2 Background and Context: Liechtenstein's "Blockchain Act"

2.1 *Object and Purpose of the Act*

Liechtenstein has broken new ground in the last few years. In 2019, the legal basis for the regulation of the Token Economy was created with the introduction of the Act on Tokens and TT Service Providers (TVTG).[3] The Act is often referred to as the "Blockchain Act", which is inaccurate, as its scope extends beyond blockchain technology. The act aims to establish a comprehensive and technology-neutral legal framework for transaction systems based on so-called "Trustworthy Technology (TT)".[4] TT means technologies through which the integrity of tokens, their assignment to Identifiers and the disposal over them is ensured.[5] Hence, the act aims to cover a broad range of applications.

To balance flexibility for innovation and legal certainty, the government of the Principality launched various initiatives and contact points to assist market participants in meeting the regulatory and legal requirements.[6] Furthermore, Liechtenstein, as an EEA-member, offers full access to the European market. These might be reasons that have made Liechtenstein a vibrant place for businesses based on new technologies.

Unlike the concepts in other jurisdictions, the Liechtenstein approach contains a part dedicated to private law issues alongside a regulatory section. On the one hand, the TVTG sets out which requirements TT Service Providers[7] must fulfil to achieve their business models and offer services in Liechtenstein. This includes registration and supervision of TT Service Providers with headquarters or place of residence in Liechtenstein.[8] On the other hand, the TVTG implements a new approach regarding the legal nature, classification

3 Law of 3 October 2019 on Tokens and VT Service Providers, Liechtensteinisches Landesgesetzblatt, 2019 No. 301 (Token and VT Service Provider Act; "TVTG"); entered into force on 1 January 2020. An English translation of the act is available at <https://www.regierung.li/law> accessed 28 June 2023.

4 *Id.* at Art. 1(1).

5 *Id.* at Art. 2(1) a.

6 For more information on the initiatives see the Office for Financial Market Innovation and Digitalization (SFID), "Innovation-Framework" (*Impuls Liechtenstein*) <https://impuls-liechtenstein.li/en/> accessed 28 June 2023.

7 On the TT Service Providers see Simon Laimer and Christian Sillaber, "VT-Dienstleister," in Judith Sild (ed), *Grundsatzfragen des liechtensteinischen TVTG* (Wien: Jan Sramek Verlag 2021), 33–67.

8 TVTG (n 3), Art. 11; see Judith Sild, "Registrierung von VT-Dienstleistern," in Judith Sild (ed), *Grundsatzfragen des liechtensteinischen TVTG* (Wien: Jan Sramek Verlag 2021), 69–92; Nicolas Raschauer and Thomas Stern, "Staatliche Aufsicht über VT-Dienstleister," in Judith Sild (ed), *Grundsatzfragen des liechtensteinischen TVTG* (Wien: Jan Sramek Verlag 2021), 131–156.

and transfer of tokens under civil law.[9] Liechtenstein has introduced the so-called "Token-Container-Model".[10] According to this model, tokens are legal objects that can represent rights of all kinds.[11] Article 7(1) TVTG stipulates that the transfer of the token results in the transfer of the right represented by the token. This basic principle requires that competing disposals over the represented rights are precluded, which is the duty of corresponding TT Service Providers.[12]

2.2 *Introduction of Uncertificated Securities Based on "Trustworthy Technologies"*

So-called "uncertificated securities" (*Wertrechte*) play an important role in the context of the representation of rights and their transfer by means of digital registers. Uncertificated securities are non-physical titles that represent a right. They are created and transferred by entry in a book, or register.[13] Before the TVTG came into force, Liechtenstein's law did not contain a statutory basis for uncertificated securities that could exist independently of a physical instrument.[14] It is no coincidence that this changed and *Wertrechte* have been introduced into Liechtenstein's law at the same time as the TVTG.[15] These are rights with the same functions as securities, whereby the functions of the physical instrument are replaced by entry into a register.[16] *Wertrechte* can be created, transferred or pledged by entry into a register, which is kept by the obligor (issuer). The core novelty is that this register may be kept and

---

9 Thomas Nägele, *Die Rechtsnatur von Token nach dem liechtensteinischen TVTG unter besonderer Betrachtung des Token-Container-Modells* (Vaduz: DLT media GmbH 2021), 30.

10 *Id.* at 35.

11 TVTG (n 3), Art. 2(1) c defines Token as "piece of information on a TT System which: (1) can represent claims or rights of memberships against a person, rights to property or other absolute or relative rights […]."

12 *Id.* at Art. 7(2) b.

13 See the corresponding Swiss terminology in Article 973c of the Swiss Code of Obligations (Federal Act on the Amendment of the Swiss Civil Code of 30 March 1911, SR 220, AS 27 317) (*Obligationenrecht*; "OR").

14 Nevertheless, uncertificated securities were not alien to Liechtenstein's law. This was also emphasised by the legislator in the Report and Motion of the Government on the TVTG, Bericht und Antrag (BuA), 54/2019, 108 ("BuA 54/2019"). See Francesco Schurr and Angelika Layr, "Emission und Übertragung von DLT-Wertrechten im internationalen Privatrecht Liechtensteins und der Schweiz," (February 2022) 121 ZVglRWiss 35.

15 § 81a SchlTPGR; See Maximilian Jörg, Angelika Layr, and Marco Lettenbichler, "Übertragung von Rechten auf VT-Systemen," in *Grundsatzfragen des liechtensteinischen TVTG*, ed. Judith Sild (Wien: Jan Sramek Verlag, 2021), 229–235.

16 § 81a(1) SchlTPGR; see *e.g.*, Angelika Layr, "Tokenization of Assets: Security Tokens in Liechtenstein and Switzerland," (2020) SPWR 121, 129.

managed using trustworthy technology.[17] *Wertrechte* can, but not necessarily have to, be represented by tokens.

The Liechtenstein legislator recognised the functional equivalence of certificated and uncertificated securities and held that entries in decentralised registers may also perform all functions of securities, which is why equal legal treatment was advocated and is now stipulated by law. The *bona fide* purchaser is protected and therefore, acquisition of rights represented by tokens by virtue of good faith is also provided for by law.[18]

2.3 *Party Autonomy: Applicability of the TVTG for Tokens Generated or Issued by Liechtenstein's TT Service Providers and Choice of Law*

For practitioners, legal certainty is of utmost relevance. Legal certainty requires the legal recognition of the issuance and transfer of blockchain-based assets and the link and legal effects on the represented assets by the applicable law. Since cross-border transactions are the standard case in a digital environment, the question arises as to how the applicable law can be determined. The Liechtenstein legislator has recognised the difficulties in finding the corresponding connecting factors and determining the law applicable to tokens. While this is the role of conflict of laws, no amendments in Liechtenstein's PIL were made during the legislative process. The TVTG declares that the civil law provisions are applicable to tokens generated or issued by a TT Service Provider which is headquartered or residing in Liechtenstein.[19] This refers to the right to the token, but not necessarily to the rights represented by it.

This approach is reminiscent of the separate connecting factors in conflict-of-laws rules of certificated securities (in the sense of "*Wertpapiere*"), in which a distinction is made between the right to the paper (*Wertpapiersachstatut*) and the right arising from the paper (*Wertpapierrechtsstatut*).[20] While the right

17 § 81a(4) SchlTPGR. Register-keeping by means of TT is no necessity for uncertificated securities; therefore, registered securities can also exist on central registers based on other technologies. Unlike the new Swiss provisions on uncertificated securities, Liechtenstein's law does not know a linguistic distinction between uncertificated securities kept by central intermediaries (*Einfache Wertrechte*; OR (n 13), Art. 973c) and ledger-based securities (*Registerwertrechte*; OR (n 13), Art. 973d).

18 TVTG (n 3), Art. 9.

19 *Id*. at Art. 3(2).

20 See, *e.g.*, Matthias Lehmann, "Internationales Privat- und Zivilprozessrecht," in Sebastian Omlor and Mathias Link (eds), *Kryptowährungen und Token* (1st edn, Recht und Wirtschaft 2021), 221; who states that this approach could also be used in the context of blockchain transactions. Disapproving due to the digital nature of Token; Andreas Kerkemeyer, "Blockchain-Transaktionen im Internationalen Recht," (2020) 184 Zeitschrift für das gesamte Handels- und Wirtschaftsrecht 739, 826.

to the paper is governed by the place of location of the security certificate, the securitised right is localised depending on the nature of the right. This would be the *lex societatis* in case of securitised shares or the *lex rei sitae* for securitised property rights.[21]

The TVTG addresses the problem of localising tokens in view of their decentralised and digital nature. It provides that if Liechtenstein's law is applicable, the token is considered to be located in Liechtenstein.[22] However, in the globalised digital world, practice must deal with tokens generated outside of Liechtenstein. For these cases the TVTG provides that the parties can expressly choose its provisions.[23] In the case of a valid choice of law in favour of Liechtenstein's law, the provisions of the TVTG will also be applicable for the disposition of blockchain-based uncertificated securities due to the reference in Article 81a(4) PGR. The choice of law seems to be the most reliable option to determine the applicable law with legal certainty.[24] It must be noted that the validity of the choice of laws must be carefully drafted and analysed, as it may be invalidated by overriding mandatory rules or *ordre public* in some jurisdictions.[25]

In the absence of an express choice of law in favour of Liechtenstein law, the correct source of conflicts of laws must be consulted to determine the applicable law on tokens generated or issued outside of Liechtenstein. The legal effect of token transfers depends on the nature of the rights represented.[26] Therefore, the consequences on the rights represented are only governed by Liechtenstein law if the applicable PIL so determines.[27] In summary, the practitioner must find the corresponding connecting factors for the specific case and right represented.[28] There are some hurdles within the Liechtenstein legal system, as Liechtenstein's conflict of laws is not exclusively regulated in a single consolidated legal text. Provisions regarding conflict of laws can be found in the Act on Private International Law (IPRG),[29] as well as in other acts

21 See below, 3.1.

22 TVTG (n 3), Art. 4.

23 *Id*. at Art. 3(2).

24 See also Lehmann (n 20), 235.

25 Cf. *id*. at 225–226.

26 See Bianca Lins and Sébastien Praicheux, "Digital and blockchain-based legal regimes: An EEA case study based on innovative legislations – comparison of French and Liechtenstein domestic regulations," (2020) SPWR 311, 318.

27 BuA 54/2019 (n 14), 69.

28 Schurr and Layr (n 14), 40.

29 Act on International Private Law (*Gesetz über das internationale Privatrecht*), LGBL 1996/194 ("IPRG"). The Act is mainly based on the Austrian IPRG; see Report and Motion

like the Persons- and Company Act (PGR).[30] In the following, the conflict of laws situation will be illustrated based on the issuance and transfer of tokens according to Liechtenstein's PIL.

3 Tokens According to Liechtenstein's PIL

3.1 *Party Autonomy: Choice of Law*

Liechtenstein's PIL is based on the principle of party autonomy, which means that parties can choose the law applicable to contractual obligations.[31] This is also valid for consumer contracts, provided that the choice of law is not disadvantageous for the consumer.[32] By contrast, a choice of law is not permitted for claims arising from the public issuance of equity or debt securities based on prospectuses and similar announcements.[33] For issues regarding corporate law or property law, the law applicable to the company or the law where the property is located shall remain reserved.

3.2 *Law Applicable in the Absence of a Choice*

3.2.1 Issuance of Tokens representing Claims

In the absence of an express choice of law, it must be examined whether the prerequisites for application of the special connecting factors of Article 40–53 IPRG are met.

Article 40 IPRG stipulates that mutual contracts under which one party owes the other at least predominantly "money" are to be assessed according to the law of the country in which the other party resides.[34] This will be the case if a party buys tokens using legal tender. This might also be argued for payments in Bitcoin and similar payment tokens. The assessment becomes more difficult for performance in other types of tokens.

Concerning the Private International Law Act and amendments to the law on persons and companies, BuA 167/1996, 2 ("BuA 167/1996").

30 The Act on Persons and Companies (*Personen- und Gesellschaftsrecht*), LGBL 1926/4 ("PGR"), contains provisions regarding international corporate law, to name one example. On the sources of law in Liechtenstein's conflict of laws, see Benedikt Jehle, *Die Schuldverträge im Internationalen Privatrecht Liechtensteins* (Schaan: GMG 2008), 31.

31 IPRG (n 29), Art. 39.

32 *Id*. at Art. 45(2).

33 See PGR (n 30), Art. 237d, which is based on Art. 156 of the Swiss Federal Act on Private International Law of 18 December 1987, SR 291, AS 1988 1776.

34 IPRG (n 29), Art. 40(1): *"Gegenseitige Verträge, nach denen die eine Partei der anderen zumindest überwiegend Geld schuldet, sind nach dem Recht des Staates zu beurteilen, in dem die andere Partei ihren gewöhnlichen Aufenthalt hat."*

Whilst the decentralised nature of blockchain-based business models may not suggest it, transactions often involve intermediaries, like banks or (crypto) exchanges.[35] Banking transactions shall be governed by the law of the jurisdiction of the establishment of the bank in operation of which the contract was concluded.[36] For the evaluation, only the nature of the transaction is of relevance, the existence of a banking license is no prerequisite for the applicability of the provision.[37] The law further stipulates that stock exchange transactions and similar contracts shall be governed by the law where the stock exchange is located.[38] According to the legislative bill, this provision does not cover transactions carried out by electronic means.[39] For such transactions, the general rule according to Article 39 IPRG – which refers to the possibility of choice of law – applies. In the absence of a valid choice of law, the applicable law will depend on the place of the characteristic performance, which must be determined in each individual case. For transactions on crypto exchanges, this will usually be the location of the exchange.[40] However, the determination of the location might pose hurdles, because of the distributed corporate structure of some crypto exchanges.

Caution is required in the case of consumer contracts. If a company carries out its activities in a country which grants special protection for consumers under private law, the law where the consumer is resident is applicable.[41] A choice of law in consumer transactions is possible but might not be considered insofar as it is disadvantageous for the consumer.[42]

If the contract does not fall into one of the categories of Article 40–53 IPRG, the closest connection of the contractual relationship must be determined. To ascertain this, all relevant circumstances of the contract – such as jurisdiction agreements, domicile, place of performance, etc. – must be considered. The contract shall be governed by the law of the jurisdiction with which it is most closely connected. This is the residence of the party who provides the characteristic performance of the contract, which is usually the party that does not owe a mere monetary payment obligation.[43] In case of the issuance of TT-based tokens, the issuer grants the power of disposal over tokens in return for payment in cryptocurrencies or legal tender. Therefore, the issuer will provide the

35 See *e.g.*, Kerkemeyer (n 20), 817–820.
36 IPRG (n 29), Art. 42(1).
37 BuA 167/1996 (n 29), 11.
38 IPRG (n 29), Art. 43.
39 BuA 167/1996 (n 29), 12.
40 See Schurr and Layr (n 14), 43.
41 IPRG (n 29), Art. 45(1).
42 *Id.* at Art. 45(2).
43 See *id.* at Art. 40, which is based on § 36 of the Austrian IPRG with the same wording.

characteristic performance of the contract, which shall then be governed by the law of the issuing party.

3.2.2 Transfer of Token Representing Claims

In the context of the transfer of tokens, the question arises as to which law determines whether a right is represented by a TT-based token and if the transfer of the token causes the transfer of the represented right, in other words, whether the right is legally tied to the token. Due to parallels to the transfer of claims by means of certificated securities, comparison with the relevant principles might be beneficial. As described above, for tangible physical security certificates a link to the location of paper can quite easily be established. The intangible and digital nature of tokens prevents their geographical localisation and complicates the determination of the connecting factors. However, this issue is not entirely new. PIL has already been challenged by the dematerialisation of securities before the invention of trustworthy technologies.[44] The intangible nature of such securities led to a shift towards the Place of the Relevant Intermediary Approach (PRIMA).[45]

This approach is also reflected in Liechtenstein's PIL. In implementation of the Directive on Financial Collateral Arrangements,[46] corresponding provisions regarding the location of so-called book-entry securities – booking and registration replacing the actual transfer and holding of a physical document – were introduced. The relevant provision (Article 37a IPRG) stipulates that the content and acquisition of rights *in rem* to these securities are governed by the law of the country in which the relevant account is maintained. The account is maintained by or on behalf of an intermediary.[47] The analogous application of this provision on the transfer of TT-based uncertificated securities is debatable. This interpretation has recently been advocated for the equally worded Austrian Article 33a IPRG.[48] However, in the absence of a central account-keeping intermediary, the question regarding the applicable

---

44 See the discussion in connection with the introduction of uncertificated securities in Switzerland; Jolanta Kren Kostkiewicz, *Schweizerisches internationales Privatrecht* (Bern: Stämpfli Verlag 2018), N 1950.

45 This approach has been adopted by the Hague Convention of 5 July 2006 on the Law Applicable to Certain Rights in Respect of Securities Held with an Intermediary; see Art. 4 of the Convention. The Convention was ratified by Switzerland, but not by Liechtenstein. See further, Schurr and Layr (n 14), 45.

46 Directive 2002/47/EC of the European Parliament and the Council of 6 June 2002 on financial collateral arrangements, [2002] OJ L168/43.

47 *Id*. at Art. 2(1) g.

48 Markus Aigner, "Das internationale Privatrecht und die Blockchain – ein unlösbarer gordischer Knoten?," (2020) 26 ZfRV 211, 220.

law would remain unanswered.[49] In the case of TT-based uncertificated securities, there is a register-keeping body to which a connecting factor can be established. According to Liechtenstein law, the obligor is responsible to keep the register (*Wertrechtebuch*). As a result, the law where the registrar is headquartered would be applicable.

For the pledge of claims Liechtenstein's PIL stipulates that the substantive law of the underlying claim shall apply.[50] Subsidiarily, the principle of the closest connection shall prevail.[51] Therefore, in absence of a choice of law, the determination of the law applicable is again dependent on the right represented.

3.2.3 Transfer of Tokens Representing Rights of Membership

In Company law, Liechtenstein follows the "incorporation theory", as evidenced by Article 232 PGR. This provides that companies are subject to the law of the state according to whose laws they are organised, *i.e.*, the law whose registration regulations they meet, or which they have declared applicable in the articles of association. Subsidiarily, the law of the place where the company has its place of effective management is applicable.[52] The law governing the company therefore is decisive for questions regarding the legal representation of membership rights by means of tokens as well as for questions regarding the transfer of such rights. This could lead to some unexpected outcome if tokens are used to represent shares and other rights of membership of foreign companies.

3.2.4 Transfer of Tokens Representing Rights to Property

Rights *in rem* (including possession) of immovable property, as well as the formal requirements for legal transactions in immovables are governed by the law of the jurisdiction in which the property is located (*lex rei sitae*).[53] The extent to which such rights can be linked to a token is to be assessed according to the *lex rei sitae* as well. The same is true for the acquisition and loss of rights *in rem* in movable objects. They are governed by the *lex rei sitae* at the time of the

49 On the difficulty of determining the relevant intermediary, cf. Lehmann (n 20), 232–233.

50 IPRG (n 29), Art. 49.

51 *Id.* at Art. 1(2); see BuA 167/1996 (n 29), 10.

52 See *e.g.*, Francesco Schurr, "Aktuelle Fragen zur Behandlung liechtensteinischer Stiftungen im internationalen Privatrecht," in Francesco Schurr (ed), *5 Jahre neues Stiftungsrecht – Unternehmensträgerschaft, Haftung, Anerkennung und Philanthropie* (Zürich: Schulthess 2017), 104. The alternate application of the "real seat theory" is also known under Swiss law; see Swiss IPRG (n 33), Art. 154.

53 IPRG (n 29), Art. 32(1) and 33.

completion of the transaction.[54] In order to be effective *vis-à-vis bona fide* third parties, property rights require the degree of publicity as the law stipulates at the place of the location.[55] Liechtenstein's law will therefore only be applicable for property located in Liechtenstein. Nevertheless, solutions in practice could be found by using a Liechtenstein structure as an intermediary.

3.3 *Prospectus Liability*

Liechtenstein's conflict-of-laws rules provide for a special connecting factor for claims arising from the public issuance of equity or debt securities based on a prospectus or similar announcement (Art. 237d PGR). These may be asserted according to the law applicable to the issuing company or under the law of the country where the issuance took place.[56] This provision has been taken over from Swiss law,[57] which is why the Swiss doctrine and case law can be referred to in this regard. Choice of law is not permitted, but the plaintiff has a right to choose between the two options.

Since the Liechtenstein legislator intended to grant equal legal treatment of (blockchain-based) uncertificated securities and certificated securities, a broad interpretation must be assumed, so that uncertificated securities are also covered by this provision. However, mere private placements with a very limited group of addressees are excluded from the scope of application.[58] Consequently, an issue on a private blockchain is generally not covered by this provision.[59] Due to the nature of the issuance by means of trustworthy technologies, the effective place of issue will be difficult to determine. For this reason, it seems appropriate to interpret the provision in a restrictive way based on teleological considerations. Consequently, the *lex societatis* of the issuing company would apply.[60]

3.4 *Blockchain-based Documents of Title to Goods* (*"Warenpapiere"*)

Documents of title to goods are negotiable instruments issued by a warehouse keeper or carrier that confer the right to demand delivery of goods. In addition, they can also represent the goods, which means that handover of the

54 *Id*. at Art. 34(1).
55 *Id*. at Art. 36.
56 PGR (n 30), Art. 237d.
57 BuA, 167/1996 (n 29), 19; see the corresponding Swiss IPRG (n 33), Art. 156.
58 See *e.g.*, Kostkiewicz (n 44), N 2967.
59 Schurr and Layr (n 14), 48.
60 *Id*.

paper instrument is deemed equivalent to the delivery of the goods themselves.[61] Furthermore, the goods may be pledged by pledging the documents.[62] When one thinks about documents of title to goods, the first thing that comes to mind are Bills of Ladings (B/L) and the like. Since Liechtenstein is landlocked between Austria and Switzerland, such instruments may *prima facie* play a subordinate role in the country. However, such documents can take on a wide variety of functions and serve to trade the goods while in transit, and can be used as collateral.[63] Therefore, instruments like B/L are essential tools in trade finance.

Digital documents of title to goods and other transport documents are important use cases for blockchain technology.[64] As the TVTG basically allows for the representation of all rights, it also allows for representation of rights to goods by tokens as a functional equivalent to negotiable instruments. In contrast to physical instruments, the determination of the location of the digital equivalent implies the hurdles already described. Again, the importance of choice of law becomes apparent.

4 Conclusion

As outlined in this chapter, Liechtenstein has introduced an innovative and comprehensive legal framework for the Token Economy, which also covers the issuance and transfer of blockchain-based uncertificated securities. The predominantly international cases require a link to a legal system that recognises the intended legal effects of the digital issuance and transfer. Not all situations can be clearly classified within the existing rules of PIL. This ultimately leads to the situation that the choice of the applicable law will be crucial to provide legal certainty. The situation in Liechtenstein seems to be particularly complicated due to the legislative fragmentation of the PIL.

---

61 Art. 504(1) of the *Sachenrecht* (Property Law, SR; LGBL 1923/4) ("SR"). Liechtenstein's Property Law has been adopted from Swiss Law. The corresponding provision in the Swiss Civil Code of 10 December 1907, SR 210, AS 24 233 ("ZGB") is Art. 925(1).

62 SR (n 61), Art. 387; see Swiss ZGB (n 61), Art. 902.

63 See *e.g.*, Marek Dubovec, "The Problems and Possibilities for using Electronic Bills of Lading as Collateral," (2006) 23 Arizona Journal of International & Comparative Law 437. On the functions see e.g., Andreas Furrer, *Schweizerisches Fracht-, Speditions- und Lagerrecht* (Bern: Stämpfli 2016), 64–65.

64 See *e.g.*, David Saive, *Das elektronische Konnossement* (Tübingen: Mohr Siebeck 2020); Niels-Philip Abdellatif, "An Ethereum bill of lading under the UNCITRAL MLETR," (2020) 27 Maastricht Journal of European and Comparative Law 250, 273–274.

CHAPTER 26

Blockchain and Japanese Private International Law

Tetsuo Morishita

1 Introduction

This chapter examines the content of Japanese law on Private International Law issues concerning transactions using blockchain technology.[1] There are a great variety of transactions, services, or systems that use or may use blockchain technologies, such as cryptocurrencies, trade finances, derivatives, non-fungible tokens, logistics, supply chain management, land registrations, healthcare, *etc*. However, it seems that the use of blockchain can roughly be divided into two categories. In the first category, as envisioned in the paper by Satoshi Nakamoto,[2] the founder of blockchain, an environment is created in which each person or entity can communicate and transact, peer-to-peer, on the internet, without relying on the management or services by central control bodies or other intermediaries. Bitcoin is one of the typical examples. As discussed in this chapter, this use of blockchain causes various challenges to PIL.

On the other hand, in the second category, while technically replacing conventional computer systems for business operations or systems with blockchain, these technologies are used in the backyard of the businesses or as a part of the systems, and there is no change in the user interfaces and the relationships between customers and business providers. For example, if financial institutions want to use blockchain instead of their conventional computer systems or networks to process data between banks to provide remittance

1 The author wrote an article in Japanese on cross-border legal issues relating to cryptocurrencies (Tetsuo Morishita, "The analysis on cross-border legal issues relating to crypto currencies" (Japanese: Kasotsuka nikansuru Kokusaitekina Hotekimondai nikansuru Kosatsu) in *Kinyuuhomu Kenkyukai, Kasotsuka nikansuru Shihojo Kantokuhojo no Syomondai no Kento* (March 2019) <https://www.zenginkyo.or.jp/fileadmin/res/abstract/affiliate/kinpo/kinpo2016_1_4.pdf> accessed 28 June 2023. This chapter is based on that article and develops the analysis there.

2 Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (*Bitcoin*) <https://bitcoin.org/bitcoin.pdf> accessed 28 June 2023.

© TETSUO MORISHITA, 2023 | DOI:10.1163/9789004514850_028
This is an open access chapter distributed under the terms of the CC BY-NC-ND 4.0 license.

services to their customers,[3] at least as far as the relationship between the financial institution and its customers are concerned, there are no significant changes. In such cases, the use of blockchain is unlikely to create new PIL issues regarding the relationship between customers and businesses, and there are no new issues regarding international jurisdiction or choice of governing law.

In addition, we should note that many services or transactions involving the use of blockchain are provided indirectly. Most individuals who own crypto-asset do not directly access the blockchain and create their own wallets to manage their private keys. On the other hand, they open accounts with intermediaries such as crypto-asset exchanges, who have direct access to blockchain and manage private keys on behalf of their customers. When considering the rights of those who directly participate in the blockchain network, the legal nature of the customers' interest in the crypto-asset would be an issue. On the other hand, when considering the rights of those who hold the crypto-asset via intermediaries, we also need to consider the legal problems arising from such indirect holdings. However, as discussed later, the latter would not cause totally new PIL issues because we could apply conventional analyses that have been developed concerning indirectly held financial assets.

2 The Use of Blockchain and PIL

In transactions, services, or systems using blockchain, cross-border legal issues easily arise, such as (1) which country has the jurisdiction to adjudicate (the issue of international jurisdiction of courts), (2) to what extent each country's criminal law and regulations should/may be applied extraterritorially (the issue of extraterritorial application), and (3) which laws should be applied (the issue of PIL in the narrow sense, or applicable laws). While there are existing legal frameworks for each issue, we need to consider whether any particular legal frameworks or considerations are required to deal with transactions, services, and systems that use blockchain.

Disputes that may arise are diverse, reflecting the variety of uses, relevant parties, and possible conflicts. Where crypto-assets are concerned, there is cryptocurrency without an issuer, such as Bitcoin, which are difficult to consider in the same way as claims, but also tokens with issuers that are used to raise funds and are similar to claims as well as tokens representing an interest

3 An example of such project is Liink by J.P. Morgan. Liink by J.P. Morgan, "Transforming how payment-related information moves" (*Onyx by J.P. Morgan*) <https://www.jpmorgan.com/onyx/liink> accessed 28 June 2023.

in other digital or tangible assets. For example, various parties are involved in transactions using blockchain, such as business entities, their customers, platform operators, application developers, hardware manufacturers and sellers, blockchain nodes, *etc.*[4] It is argued that in a genuinely decentralised environment using blockchain, the traditional actors who have been subject to regulations, for example, intermediaries as banks, will disappear, and it will be necessary to consider alternative addressees for effective regulations, for example, end-users, internet service providers, search engines and social networking sites, wallets providers, miners, software producers, and hardware manufacturers. In addition, there may be various types of disputes such as claims for damages or specific performance for breach of contract, damages for tortious acts, or claims based on property rights such as the return of assets. Considering the importance of technologies and difficulties in finding and identifying parties typically targeted as defendants in conventional transactions not using blockchain, parties that were not typical defendants in the past may be targeted by plaintiffs.

Accordingly, the legal frameworks to be applied and the issues to be considered regarding jurisdiction, extraterritorial application, and applicable law will differ depending on how blockchain is used, the type of transactions, the parties involved, and the kind of issues. The following sections examine jurisdiction, extraterritorial application, and applicable law, in that order. The examination will focus on crypto-assets, where the practical use of blockchain is most advanced, and other examples of practical uses of blockchain will be mentioned when necessary.

3 International Jurisdiction of Japanese Courts

3.1 *Japanese Law on International Jurisdiction*

According to the rules of international jurisdiction stipulated in Japan's Code of Civil Procedure,[5] Japanese courts have general jurisdiction, which allows

4 Primavera De Filippi and Aaron Wright, *Blockchain and the Law* (Harvard University Press 2018), 173–184.

5 Japan's Code of Civil Procedure was amended in 2011, and the provisions on international jurisdiction of Japanese courts were newly introduced (before that, there was no express provisions on international jurisdiction of Japanese courts in civil cases). The English translation of Japan's Code of Civil Procedure is available at The Ministry of Justice, "Japanese Law Translation," (*Japanese Law Translation*) <http://www.japaneselawtranslation.go.jp/?re=02> accessed 28 June 2023.

for any kind of action, and special jurisdiction, which only allows for specific actions.

Japanese courts have general jurisdiction only over corporations with their principal office or place of business in Japan (Article 3–2, Paragraph 3 of the Code of Civil Procedure); they do not have general jurisdiction over corporations with head offices in foreign countries. Special jurisdiction likely to be relevant to transactions using blockchain includes jurisdiction over: (1) an action for a claim related to a contractual obligation (if the contractually specified place of performance of the obligation is in Japan, or if the place of performance is in Japan according to the governing law of the contract that is chosen in the contract) (Article 3–3(1) of the Code of Civil Procedure); (2) an action regarding property rights (if the subject matter of the claim is located within Japan, or if the action is a claim for the payment of monies, and seizable property of the defendant located in Japan (except when the value of such property is extremely low)) (Article 3–3(3) of the Code of Civil Procedure); (3) an action against a person that conducts business in Japan (if it involves the business that the person conducts in Japan) (Article 3–3(5) of the Code of Civil Procedure); and, (4) an action in tort (if the place where the tort occurred is in Japan[6] (except if the consequences of a wrongful act committed in a foreign country have arisen in Japan but it would not ordinarily have been possible to foresee those consequences arising in Japan)) (Article 3–3(8) of the Code of Civil Procedure). If there is an agreement on jurisdiction, the agreement is respected in principle.[7] However, the agreement is not valid unless it is made regarding actions that are based on a specific legal relationship and executed by means of a paper document or electronic or magnetic record (Article 3–7 (1)(2) of the Code of Civil Procedure). In addition, concerning consumer contracts, special rules are applied from the perspective of consumer protection (Article 3–4, Paragraphs 1 and 3, Article 3–7, Paragraph 5).

3.2 *Blockchain and Jurisdiction*

There are neither statutes that specifically address the jurisdiction of Japanese courts dealing with civil cases involving blockchain nor court cases regarding

6 "The place where the tort occurred" includes the place where a tortious act is committed as well as the direct result of the tortious act occurred. Masato Dogauchi, Introduction to Private International Law (Japanese: *Kokusai Shiho Nyumon dai 8 han*) (8th edn, Yuhikaku 2018), 280.

7 It is the established case law and the dominant theory that when the agreement on jurisdiction is extremely unreasonable and against the public policy, such agreement would be ineffective (Supreme Court, Judgment on 28 November 1975, 29 Minshu No. 10, 1554).

jurisdiction of Japanese courts in civil matters relating to transactions using blockchain technology. International jurisdiction in civil litigation related to transactions using blockchain technology depends on the identity of parties and the matter in dispute. While the rules of international jurisdiction, as described above, are likely to work well in many cases concerning blockchain-based transactions, there are still several points that may raise challenging issues.

First of all, it should be noted that it would often be challenging to identify and locate the appropriate defendant because of the pseudonymity of blockchain.[8] Though participants on the blockchain could all be recorded on the chain, transactions on the chain may be made with digital signatures and public-private key systems without revealing a true identity.[9] For example, if a crypto-asset is stolen by someone in the blockchain network, it might be hard for the aggrieved party to identify the person who has stolen the crypto-asset or who is holding the stolen asset.[10] If the person who has stolen or is holding the stolen asset cannot be identified, the aggrieved party would have difficulty filing a lawsuit.

Also, proving the facts recorded on a blockchain could be a practical challenge. Article 247 of Japan's Code of Civil procedure stipulates, "[i]n reaching a judgment, the court decides whether to find allegations of fact to be true based on its freedom of personal conviction, in light of the entire import of oral arguments and the results of the examination of evidence," and judges have discretion in terms of the evaluation of evidence. Though an electronic form of evidence is acceptable in a Japanese court, how the record on the blockchain could be submitted to a court in such a manner as judges could see, read, and recognise would be an issue.[11]

---

8 Souichiro Kozuka, "Smart Contract and Private International Law" (Japanese: Smart Contract to Kokusai Shiho) (2021) 57 Gakushuin Daigaku Hogakukai Zasshi 1, 11.

9 Filippi and Wright (n 4), 38.

10 Though it is not easy to identify the persons who are holding the stolen crypto-asset, it is not impossible. For example, in March 2020, the Japanese police arrested two Japanese who knowingly acquired a part of Yen 58 billion worth of NEM that were stolen in January 2018 from Coincheck, a Japanese crypto exchange. The Japan Times, "Tokyo police arrest two for receiving stolen NEM cryptocurrency" (*The Japan Times*, 11 March 2020) <https://www.japantimes.co.jp/news/2020/03/11/national/crime-legal/tokyo-police-arrest-two-taking-possession-stolen-nem-cryptocurrency/> accessed 28 June 2023.

11 International Swaps and Derivatives Association (ISDA), Linklaters, and R3, "Private International Law Aspects of Smart Derivatives Contracts Utilizing Distributed Ledger Technology: Japanese Law" (*ISDA*, October 2020), 11 <https://www.isda.org/a/FCrTE/Private-International-Law-Aspects-of-Smart-Derivatives-Contracts-Utilizing-DLT-Japanese-Law.pdf> accessed 28 June 2023.

Next, suppose an agreement on jurisdiction concerning a transaction using a blockchain is made between the parties participating in that transaction in a contract that is separate from the blockchain itself. In that case, such an agreement on jurisdiction will be respected in disputes arising from the transaction using the blockchain. For example, ISDA (International Swaps and Derivatives Association) has published legal guidelines for smart derivative contracts using blockchain technology (derivative contracts in which some terms can automatically be performed by using the blockchain).[12] The ISDA smart derivative contracts use Corda blockchain and the smart contract platform developed by R3 (a company providing a distributed ledger technology platform). The parties to ISDA smart derivative contracts will enter into the ISDA Master Agreement as well as an agreement with a platform provider.[13] In such arrangements, the clauses on jurisdiction will be respected in disputes among the parties to the agreements under Article 3–7 (1) of the Code of Civil Procedure. Even though there is no agreement regarding jurisdiction in the relevant agreement relating to a smart contract, if the smart contract is used as a tool to perform another contract among the parties and there is a jurisdiction clause in the latter contract, the agreement regarding jurisdiction in the latter would be considered to cover disputes relating to the smart contract.[14] A code of the blockchain could contain a stipulation about dispute resolution. However, if it is difficult to expect standard participants (the level of sophistication of the participants may differ depending on the type of the system) to recognise and understand the content of the stipulation, such stipulation would not bind parties who have not been aware of the stipulation. The mere participation in the blockchain network should be insufficient to automatically find that there is an agreement on jurisdiction (the same could be said regarding applicable law).

When there is no agreement on jurisdiction, or disputes arise between parties without contractual relationships, and the defendant is not a person or entity with its principal place of business in Japan, we need to consider if the Japanese courts have special jurisdiction. As mentioned, Japanese courts have special jurisdictions over actions against parties conducting business in Japan

12 ISDA, "ISDA Legal Guidelines for Smart Derivatives Contracts: Introduction" (*ISDA*, January 2019) <https://www.isda.org/a/MhgME/Legal-Guidelines-for-Smart-Derivatives> accessed 28 June 2023, and ISDA, "ISDA Legal Guidelines for Smart Derivatives Contracts: The ISDA Master Agreement" (*ISDA*, February 2019), <https://www.isda.org/a/23iME/Legal-Guidelines-for-Smart-Derivatives-Contracts-ISDA-Master-Agreement.pdf> accessed 28 June 2023.

13 ISDA, Linklaters, and R3 (n 11), 5–8 for uncollateralised transactions, 14–16 for collateralised transactions.

14 Kozuka (n 8), 11 suggests such possibility.

(Article 3–3(5) of the Code of Civil Procedure); the defendant does not have to be present in Japan. This special jurisdiction was introduced to address foreign corporations doing business in Japan using information technology and the internet but without establishing offices in Japan.[15] Therefore, if a service using blockchain is provided via the internet and a person wants to commence litigation in Japan, this special jurisdiction would be relevant.

Whether or not a company is doing business in Japan is left to the findings and evaluation of the facts of each case, but if, for example, the company's website is in Japanese, most scholars would argue that it should be regarded as doing business in Japan, unless there are particular circumstances such as a system that prevents transactions from Japan. On the other hand, in the case where Japanese is not used on the company's website, various circumstances such as the possibility of actual applications from Japan, the record of transactions, and the nature of the products and services will be taken into account.[16] Otherwise, it may not be easy to determine the place of performance. Also, it may be difficult to determine the location of property or place of a tortious act in a transaction using blockchain technology.

Regarding other grounds for Japanese courts to have special jurisdiction, the question is how to determine location such as "place of performance of obligations" (Article 3–3(1) of the Code of Civil Procedure), "location of property" (Article 3–3(3) of the Code of Civil Procedure), and "place of tort" (Article 3–3(8) of the Code of Civil Procedure) in transactions and systems using blockchain technology. If a contract relating to a transaction using blockchain technology specifies the place of performance, it will be easier for Japanese courts to claim special jurisdiction over the case than if no such place is specified.

Rather than relying on the location of nodes, servers, and private keys, location should be determined considering the purpose of the relevant provisions and based on the actual situation and economic substance of transactions. In making such a determination, it is important to take into account that under Japan's current rules of international jurisdiction, even in cases where Japan's international jurisdiction is recognised, an action may be dismissed if there are "special circumstances" that prevent the case from being heard in Japan from the perspective of equity between the parties and the appropriateness and speed of the hearing (Article 3–9 of the Code of Civil Procedure). It would be preferable to determine, relatively loosely, whether or not the "place of

15 Masato Dogauchi, "New Japanese Rules of International Jurisdiction: General Observation" (2012) 54 Japanese Yearbook of International Law 260.

16 Mikio Akiyama et. al., Commentary on Civil Procedure Law, Vol. 1 (Japanese: *Konmentaru Minji Sosyoho I, dai 3han*) (3rd edn, Nihon Hyoronsya 2021), 120–121.

performance," "location of the property," or "place of the tortious act" is in Japan and then use "special circumstances" to achieve a balanced conclusion.[17]

For example, it is argued that, in the transactions of digital assets, the place of residence of the recipient could be considered as "the place of performance of an obligation," and where tokens are stolen by hacking, the residence of the most recent token holder who is a victim could be considered as the place of the tortious act.[18] This view is commendable in that it does not get overly caught up in the mechanics of using blockchain and the internet but instead focuses on the parties and objects in the real world that are substantially at issue in the dispute in order to determine jurisdiction. From the same perspective, for example, if a token represents a real-world object and a dispute arises with respect to the token, it would be reasonable to focus on the location of the real-world object in determining the place of performance, the location of the property, or the place of tort.

4 Extraterritorial Application of Japanese Law

Because transactions conducted on the internet using blockchain technology inevitably cross over national borders, they raise the issue of extraterritorial application of various criminal and public regulations.

4.1 *Criminal Law*

In the field of criminal law, the international scope of application of criminal law must be defined by statute under the principle called "nulla poena sine lege" (Article 31 of the Japanese Constitution). Under Japanese law, if a person has knowingly received proceeds of a crime, he/she shall be punished (Article 11 of Act on Punishment of Organized Crimes and Control of Proceeds of Crime). After Coincheck (a Japanese cryptocurrency exchange) was hacked by someone and cryptocurrency called NEM,[19] worth 58 billion yen, was stolen,

17 For example, in a lawsuit for damages based on tort by a Japanese plaintiff who claimed to have been defamed by an article posted on an internet website by the defendant, a Nevada corporation, the Tokyo District Court held that the place of the result of the tort was in Japan based on the fact that the website was accessible in Japan, and that there were special circumstances that a Japanese court should not conduct a trial in order to achieve equality between the parties and a fair and speedy trial (The Judgment of Tokyo District Court on 21 October 2013, 70 Minshu No. 3, 890). The judgment was supported by the Supreme Court.

18 Kozuka (n 8), 12.

19 See *supra* (n 10).

some Japanese nationals knowingly received proceeds of the crime: there are two lower court cases where they were found guilty of receiving proceeds of crime.[20]

The first issue was whether the NEM received was considered "proceeds of crime" under the Japanese Penal Code. Under the Japanese Penal Code, hacking a computer (inputting false data or giving unauthorised commands to a computer) and stealing assets is punishable as computer fraud (Article 246-2 of the Japanese Penal Code).[21] Under the Penal Code, if the person committing the computer fraud is a Japanese national, the law applies not only to crimes committed within Japan but also to crimes committed outside Japan. However, if the person is not a Japanese citizen, the law applies only to crimes committed in Japan (Article 1 and 3 of the Japanese Penal Code). The prevailing view in Japan is that a crime can be said to have been committed in Japan not only when the act takes place in Japan but also when the consequence, which is one of the necessary elements of the crime, occurs in Japan.[22]

In two cases in which persons were indicted for computer fraud after receiving part of the stolen NEM, the defence counsel argued that the crime of computer fraud could not be applied because it was not clear whether or not hacking took place in Japan. Both judgments found that there was computer fraud under the Japanese Penal Code. In this case, it was unclear where the false data had originated; however, both judgments ruled that the evidence showed that the result of the computer fraud had occurred in the place where the nodes that shared the false information were located and that at least one of the nodes that had shared the false information

20 Judgement of Tokyo District Court on March 24, 2021 (Reiwa 2 nen (toku wa) No. 885, Reiwa 2 nen (toku wa) No. 1565, Reiwa 2 nen (toku wa) No. 2168), Judgment of Tokyo District Court on 8 July 2021 (Reiwa 2 nen (toku wa) No. 884, Reiwa 2 nen (toku wa) No. 1158, Reiwa 2 nen (toku wa) No. 1373, Reiwa 2 nen (toku wa) No. 1661, Reiwa 2 nen (toku wa) No. 2199, Reiwa 2 nen (toku wa) 2456).

21 Article 246-2 of the Japanese Penal Code stipulates, "a person who illegally obtains or causes another person to illegally obtain a profit by creating a false electronic or magnetic record relating to acquisition, loss or alteration of property rights by inputting false data or giving unauthorised commands to a computer utilised for the business processes of another person, or by putting a false electronic or magnetic record relating to acquisition, loss or alteration of property rights into use for the business processes of another person, is punished by imprisonment for not more than 10 years."

22 Atsushi Yamaguchi, Criminal Law, General Issues (Japanese: *Keiho Souron dai 3 han*) (3rd edn, Yuhikaku 2016), 416. Hitoshi Otsuka, et. al., Large Commentary on Criminal Law (Japanese: *Dai Konmentaru Keiho dai 3 han dai 1 kan*) (3rd edn, Seirin Shoin 2015), vol. 1, 83.

was located in Japan. So, it was concluded that computer fraud was committed in Japan.

These judgments appear to be too technical. Following the reasoning adopted in these cases, the consequences of an act that affects the records of the blockchain would occur everywhere in the world where the nodes of the blockchain exist. However, such a view seems to recognise too widely the place where the results of the act have occurred. In this case, elements of the crime were that the criminal created a false record in a computer in order to obtain a profit. However, it was unclear where the criminals created the false record and where the profit was received. So, the above view may have been an unavoidable process to avoid leaving fraudulent activities unaddressed under the current law and to lead to a reasonable result. However, it would be more reasonable to have a legal framework allowing for the recognition of loss of virtual assets held by a party as a crime constituting element,[23] and to look into the location of the party who suffered the loss to check the territoriality of the crime.

4.2 *Extraterritorial Application of Regulations*

Among blockchain-based transactions, there are various regulations, especially regarding the trading of crypto-assets. For example, in Japan, there are regulations on crypto-asset exchanges, financial instruments trading regulations on investment tokens and derivatives trading of crypto-assets, and prohibitions of unfair trading of crypto-assets and derivatives trading using crypto-assets.[24] As transactions of crypto-assets are easily conducted across national borders, it is important to apply these regulations extraterritorially in an appropriate manner to protect Japanese customers and investors and ensure fairness of transactions of crypto-assets in Japan.

In considering the extraterritorial application of regulations, there are three issues to be considered: (1) the extent to which extraterritorial application is permitted under international law (*i.e.*, whether an extraterritorial application will violate international law), (2) as a matter of each country's law, whether individual regulations should be applied extraterritorially to achieve the purpose of the relevant regulations within the framework of international law,

23 In these cases, the defence counsel argued that cryptocurrency is not a property right, but both judgments rejected this argument and ruled that cryptocurrency is a property right in the context of Article 246-2 of the Penal Code.

24 On regulations relating to crypto-assets in Japan, Takeshi Nagase, Tomoyuki Tanaka, and Takato Fukui, "Japan," in Josias N. Dewey (ed), *Blockchain & Cryptocurrency Regulation 2022 Fourth Edition* (4th edn, Global Legal Group 2021), 334–343 <https://www.amt-law.com/asset/res/news_2021_pdf/publication_0023819_ja_001.pdf> accessed 28 June 2023.

and (3) how to practically apply the regulations extraterritorially and ensure the effectiveness of the regulations.

4.2.1 International Law

When assessing the extent to which a country can apply its own laws to matters that have an international scope, there are various theories of jurisdiction: the territoriality principle, the personal jurisdiction principle or even the effect theory.[25] In this day and age where transactions using the internet, *etc.*, are very common, it is not appropriate to be bound too much by the principle of territoriality. It is permissible and necessary under international law to appropriately regulate acts committed outside Japan if they have strong relevance to Japan and if there is a need and justification for regulation.[26] On this basis, in case regulations of multiple countries are applied, it will be important to develop ways to avoid excessive regulatory burdens. For example, the use of substituted compliance – where transactions are allowed to be conducted without being subject to the host country's regulations, provided that the home country's regulations and the host country's regulations are substantially similar – will be an important form of co-operation among authorities.

4.2.2 Necessity of Extraterritorial Application of Regulations

Where a business operator is based outside Japan and conducts securities transactions targeting domestic investors, the prevailing view favours the extraterritorial application of financial regulations. In other words, to protect domestic investors, Japanese laws and regulations should in principle be

25 Hironobu Sakai et al., International Law (Japanese: *Kokusai Ho*) (Yuhikaku 2011), 88–93.

26 With regard to the extraterritorial application of securities regulations in relation to ICOs, there is an article analysing the applicability of the regulation using the framework of three standards; the place-of-conduct standard, the place-of-effect standard, and the place-of-transaction standard. Koji Takahashi, "Jurisdiction to prescribe of Securities Regulations and ICO (Initial Coin Offering" (Japanese: Shoken Kankei Hoki no Kiritsu Kankatsuken to ICO (Initial Coin Offering)) (2019) 117-4 Kokusaiho Gaiko Zasshi 1. This paper argues that, in relation to the regulation of solicitation, while the application of the place-of-conduct standard and the place-of-effect standard to the ICO is possible, the application of the place-of-transaction standard to the ICO and the place-of-effect standard in relation to the market manipulation regulation raises the problem that it is difficult to specify the place of transaction or the place of effect. Even if it is true that there are cases where it is difficult to determine a single place of transaction or place of effect in relation to the ICO, it is sufficient to consider whether Japan has jurisdiction to prescribe based not only on the territoriality principle but also on the effect theory in considering whether Japanese law can be applied extraterritorially. In other words, it seems to be sufficient to examine whether a certain act has been done in Japan or whether an effect has been caused in Japan to the extent that a genuine linkage with Japan can be recognised.

applied to conduct that actively reaches out to local customers, even if the conduct itself is conducted outside Japan.[27]

Regarding transactions using blockchain, it may be necessary to apply the regulations extraterritorially if they actively reach out to domestic parties beyond a certain level or have a certain level of effect in Japan. Considering the variety of transactions, it is not easy to set a clear standard as to how much activity or effect is required for extraterritorial application of regulations. It will be necessary to formulate a certain standard by accumulating judgments based on the purpose of regulation and the actual conditions of individual transactions using blockchain, while referring to examples of extraterritorial application in other transactions.

4.2.3 Extraterritorial Application of Regulations on Crypto-Asset Exchanges

Under Japanese law, a person who intends to engage in Crypto-asset Exchange Service shall register with the Prime Minister and be subject to various regulations (Article 63-2 of Payment Service Act).[28] Regarding the extraterritorial application of Japanese regulation of crypto-asset exchanges in foreign countries, Article 63-22 stipulates, "[f]oreign Crypto-asset Exchange Service Providers not registered under Article 63-2 must not conduct solicitation of a person in Japan for the acts set forth in the items of Article 2, paragraph (7) (Note: Crypto-asset Exchange Service)." Since a blanket ban on cross-border transactions is inappropriate because it would reduce user convenience, this provision is intended to protect users from making transactions with foreign business providers unregulated under Japanese law because they have been solicited, although those who voluntarily use the Internet to conduct cross-border transactions without being solicited will not be subject to protection.[29]

---

27 Kinyuho Iinkai, "Interim Discussion Paper on Cross-border Application of Financial Laws and Regulations: Focusing on the Securities and Exchange Law" (Japanese: Kinyukan-renhourei no cross-border tekiyo nikansuru Chukan Rontenseiri – Shoken Torihikiho wo Chushin ni) (*Kinyuho Iinkai*, 2002), 7 <http://www.flb.gr.jp/jdoc/publication11-j.pdf> accessed 28 June 2023.

28 The Crypto-asset Exchange Service is defined as carrying out one of the following acts as its business: (i) purchase and sale of a crypto-asset or exchange with another crypto-asset, (ii) intermediary, brokerage or agency services for the act set forth in (i), (iii) management of users' money, carried out by persons in connection with their acts set forth in (i)(ii), and (iv) management of Crypto-asset on behalf of another person. (Article 2(7) of the Japanese Payment Service Act (Act No. 59 of June 24, 2009)).

29 Yasufumi Takahashi, Detailed explanation: Law on Payment Services (Japanese: *Shosetsu Shikin Kessai nikansuru Hosei*) (Kinyuzaiseijijo Kenkyukai 2010), 259.

Regarding the concrete standard to determine whether the solicitation of a person in Japan is made, the administrative guidelines of Financial Services Agency stipulate that the act of a foreign crypto-asset exchange service provider posting advertisements, *etc.* on its website, *etc.* regarding transactions related to the crypto-asset exchange service constitutes the act of "solicitation" in principle, except in cases where the website clearly shows that the service is not provided to a person in Japan or where the service provider takes necessary measures not to transact with a person in Japan, such as by checking the location of its customers.[30]

The idea expressed in the administrative guidelines is that a website may be subject to the regulations even if it is not in the Japanese language, as long as it is made available to Japanese people. At first glance, it seems questionable whether such a broad extraterritorial application can be based on the principle of territoriality. However, suppose there are or are expected to be many individuals residing in Japan who have viewed the website. In that case, it is possible to consider that the solicitation has been made in Japan and find a basis for application of Japanese laws following the territoriality principle, or to consider that the effect of the business activities using the website has occurred in Japan and find a basis for jurisdiction of the Japanese courts following the effect theory.

There are no provision on penalties for violations of Article 63-22. It is envisaged that if Japanese customers actually solicited by a foreign entity, the effectiveness of the regulation will be ensured by FSA's notifying the home country authorities that the service provider is engaged in illegal activity in Japan, encouraging them to supervise the service provider.[31] Furthermore, as a result of this approach of ensuring the effectiveness of regulations through co-operation with home country authorities, foreign service providers that are not subject to supervision by foreign authorities under a similar registration system in the foreign country are exempted from the regulations mentioned above on solicitation of persons in Japan, as it is difficult to ensure the effectiveness of regulations.[32] However, a person who conducts unregistered crypto-asset exchange services in Japan is subject to imprisonment for not more than three years or a fine of not more than three million yen (Article 107 (5) of Payment Service Act).

---

30 Kinyucho, "Administrative Guideline for Financial Companies, Chapter for Crypto Asset Exchange Service Providers" (Japansese: Jimu Gaidorain: Kinyukaisya Kankei, Angosshisan Kokangyosha Kankei) (*FSA*, June 2021), II-5-2 <https://www.fsa.go.jp/common/law/guide/kaisya/e016.pdf> accessed 28 June 2023.

31 Yasufumi Takahashi, Article by article Explanation, Payment Services Act (Japanese: *Chikujo Kaisetsu Shikin Kessaiho* (Kinyuzaiseijijo Kenkyukai 2010), 205.

32 *Id.*, 205–206.

4.2.4 Effectiveness of Regulation

Even if Japan's regulations are applied to foreign service providers, it is not easy to make the regulations effective against foreign service providers that do not have a base in Japan. The FSA has issued warnings to fifteen foreign businesses for conducting crypto-asset exchange service to Japanese residents via the Internet without registering as Crypto-asset Exchange Service Providers in Japan,[33] but it is not clear whether these foreign service providers have responded in good faith.

In its Investor Bulletin: Initial Coin Offering published in 2017,[34] the U.S. Securities and Exchange Commission (SEC) also noted the following challenges with virtual currencies for law enforcement: (1) tracing money is more difficult because traditional institutes such as banks are not involved, (2) obtaining information is more difficult because the transactions and uses span the globe, (3) it is difficult to get information because there is no one central authority, and (4) it is difficult to freeze assets or detain assets because virtual currency wallets are encrypted, and virtual currencies are not held by a third-party custodian.

Cooperation between regulators in different countries is essential to increase the effectiveness of regulations on crypto-assets. A report published in December 2018 by the FSA's Study Group on Virtual Currency Exchange Business, *etc.*, also points out that "transactions relating to virtual currencies can easily be conducted cross-border via the Internet, so there are limits to what can be done by one country alone, and international cooperation is considered essential."[35] It is hoped that Japan, which has plenty of experience in regulating virtual currencies, will actively contribute and promote international cooperation.

---

33 Blockchain Laboratory Limited (Macao) on 13 February 2018), Binance (Hong Kong on 23 March 2018, SB101 (Gibraltar) on 15 February 2019, Cielo EX Ltd (Seychelles) on 25 June 2019), BtcNext Company Limited (St. Vincent and the Grenadines) on 13 December 2019, BASE FINTECH LAB LLC (Azerbaijan) on 21 January 2020, AMANPURI Co., Ltd (United States or Malta) on 26 June 2020, Bitforex Limited (Seychelles) on 26 June 2020, Bybit Fintech Limited (Singapore) on 28 May 2021, Binance Holdings Limited (Unknown) on 25 June 2021, Vanlancle (Unknown) on 25 February 2022, Bitforex Limited (Seychelles) on 31 March 2023, Bybit Fintech Limited (Singapore) on 31 March 2023, MEXC Global (Singapore) on 31 March 2023 and Bitget Limited (Singapore) on 31 March 2023. The countries are those mentioned in the warning issued by FSA (FSA warnings say the information about the places of service providers are based on the information available on internet).

34 U.S. Securities and Exchange Commission, "Investor Bulletin: Initial Coin Offerings" (*SEC*, 25 July 2017) <https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_coinofferings> accessed 28 June 2023.

35 Financial Services Authority, "Report of the Study Group on Virtual Currency Exchange Business, etc." (*FSA*, December 2018), 32 <https://www.fsa.go.jp/news/30/singi/20181221-1.pdf> accessed 28 June 2023.

5 Applicable Law

There are neither legal provisions specifically addressing applicable law with respect to blockchain transactions nor court cases regarding the law applicable to such transactions.

5.1 *Contracts*

There are various possible legal issues related to transactions using blockchain technology. For example, suppose a dispute arises regarding a contract using blockchain technology. In that case, the governing law will be determined in accordance with the provisions of Article 7 (parties may choose the applicable law to contracts), Article 8 (in the absence of choice by parties, the law of the place that is most closely connected is applied, and the location of business of the party that provides a characteristic performance is presumed as the place that is the most closely connected), Article 11 (in case of a consumer contract, consumers may invoke the application of mandatory law of its habitual residence) of the Act on General Rules for the Application of Laws.[36]

If an agreement on choice of law regarding a contract using blockchain technology is made between the parties to the contract, the law chosen by the parties should be applied to not only the contractual issues relating to the contract but also to issues relating to the blockchain as far as they concern the parties to the contract.[37] It may be possible to write some stipulations regarding the applicable law on the blockchain,[38] however, if it is difficult to expect standard participants (the level of sophistication of the participants may differ depending on the types of the system) to recognise and understand the content of the stipulation, such stipulation would not be considered as an effective choice of law by those who have not been aware of such stipulation. On

36 The main source of PIL of Japan is the "Act on General Rules for Application of Laws" that was enacted in 2006 and which drastically changed the prior legislation. The PIL rules on contract are similar to those in Europe and Article 8 (the rule that is applied when there is no choice by the parties) adopts the concept of characteristic performance. Yoshihisa Hayakawa, "General Rules on Contract" (2007) 50 The Japanese Annual of International Law 25, 35–37.

37 Kozuka (n 8), argues that if there is a non-virtual contract, and smart contract is used as a tool to perform the non-virtual contract, the agreement on applicable law in the non-virtual contract should be interpreted to cover the disputes relating to the smart contract. *Id*., 17. ISDA, Linklaters, and R3 (n 11) agrees that Japanese court would give effect to the parties' express choice under the ISDA Master Agreement relating to contractual law issues relating to the derivative transactions using blockchain under the ISDA Master Agreement.

38 Kozuka (n 8), 17.

the other hand, the choice of applicable law may be implied.[39] Suppose, for example, there is a strong link between the record on the blockchain and other assets such as real property, personal claim or digital assets. In such case, we may find implied choice of the location of tangible assets, the governing law of the personal claim, or the applicable law to the digital asset (if such law is clearly identified) as the governing law of the contract.

When there is no choice of applicable law by the parties, the law of the place of business of the party that provides characteristic performance would be applied unless there is a place that is more closely connected to the act. It has been pointed out that in a contract where a token is delivered in exchange for cryptocurrency regarded as a means of payment, the characteristic performance is made by the person who provides the token. It is argued that, if the cryptocurrency is regarded as a thing, the contract becomes an exchange contract and characteristic performance is not an issue.[40] Although the legal nature of virtual currency is an issue under both private law and supervisory law, the question of whether or not a characteristic performance has occurred should depend not on the legal nature of the virtual currency, but on whether or not the parties to the transaction are focusing on the unique nature of the virtual currency. Also, if there is a close connection between the record on the blockchain and some assets in the real world, the location of such assets may be considered as the most closely connected place to act.

5.2 *Torts*

Article 17 of the Act on General Rules for the Application of Laws stipulates, "the formation and effect of a claim arising from a tort are governed by the law of the place where the result of the wrongful act occurred; provided, however, that if the occurrence of the result at the relevant place was ordinarily unforeseeable, the law of the place where the wrongful act was committed governs." The place where the result of the wrongful act occurred is the place where the direct result of the wrongful act occurred. There are special rules regarding product liability (the law of the place where the victim received the delivery of the product) (Article 18) and defamation (the law of the victim's habitual residence) (Article 19). If there is a place to which the tort is obviously more closely connected than the place indicated in the preceding three Articles, for example, as relevant parties have their habitual residence in the same jurisdiction or the tort was committed in breach of the obligation under the contract

39 Takao Sawaki and Masato Dogauchi, Introduction to Private International Law (Japanese: *Kokusai Shiho Nyumon, dai 8 han*) (8th edn, Yuhikaku 2018), 179.

40 Kozuka (n 8), 18.

between the parties, the law of that place is applied (Article 20). In addition, the parties to a tort may, after the tort occurs, change a law applicable to the formation and effect of a claim arising from the tort (Article 21).[41]

If property recorded on a blockchain is stolen as a result of illegal access to the blockchain by a hacker, where is the place where the result of the tortious act occurred? In the judgments mentioned above of the Japanese court on criminal cases,[42] the result of the illegal act occurred at the location of the node where the records made as a result of the unlawful access were shared. However, when blockchain is used as a tool for recording and processing data and programs, the result of unauthorised access should be considered to have occurred at the location of the property or the business to which the data and programs relate, rather than at the location of the node. So, for example, if a foreign hacker steals someone's crypto-asset, the place where the result occurred should be the location of the holder of the crypto-asset, not the nodes.[43] If the blockchain is used to record the interest in a real asset, the location of the asset should be considered as the place where the result occurred.

5.3 *Property Law*

A particular difficulty arises regarding property law issues relating to property recorded on the blockchain. Article 13 of the General Rules Law on the Application of the Law of Japan provides that "(A) real right to movables or immovables and any other right requiring registration are governed by the law of the place." As indicated in this article, the idea of applying the law of location (*lex situs*) has traditionally been adopted for property rights, but it is not easy to recognise a physical location concerning digital assets, typically crypto-assets, recorded on a blockchain.

For example, a report on distributed ledger technology (DLT) and governing law published by the Financial Market Law Committee points out that the application of the *lex situs* would be problematic in the context of DLT and gives rise difficulty in answering the following questions, "(a) what are the legal nature and effects against third parties of a disposition of an asset recorded on a DLT system?, (b) What are the requirements-if any-for the perfection of a disposition of an asset recorded on a DLT system?, (c) What are

41 Regarding the general explanation about the Japanese PIL rule on tort, see Yasushi Nakanishi, "Torts" (2007) 50 The Japanese Annual of International Law 60.

42 See *supra* (n 20).

43 Kinyuho Iinkai, "Discussion Paper on Private Law Aspects of Virtual Currencies" (Japanese: Kasotsuka no Shihojo no Ichizuke nikansuru Ronten Seiri) (*Kinyuho Iinkai* 2018), 12 (footnote 32) <http://www.flb.gr.jp/jdoc/publication55-j.pdf> accessed 28 June 2023.

the requirements-if any-for the realisation of an interest in an asset recorded on a DLT system?, (d) Does a disposition of an asset recorded on a DLT system extend to entitlements to dividends, income, or other distributions, or to redemption, sale or other proceeds?, (e) What are the legal nature and effects against the transferor of a disposition of an asset recorded on a DLT system?, and (f) What are the circumstances in which a person's interest in an asset recorded on a DLT system will extinguish or have priority over another person's interest?"[44]

About property law issues related to assets recorded on blockchains, there are three issues: (a) the relationship between interest in assets and the record of blockchains, (b) issues in transactions through intermediaries such as cryptographic asset exchanges, and (c) connecting factors when considering property law issues related to blockchains. These three issues will be discussed in turn.

5.3.1 The Relationship between Interest in Assets and the Record of Blockchain

Blockchain technology may be used to record the belongings and transfers of assets/values, and tokens relating to the assets/values are digitally issued on the blockchain. There are a variety of tokens. From the viewpoint of the functions, tokens are typically categorised into payment tokens (exchange tokens), investment tokens (security tokens), and utility tokens.[45] However, more important for PIL is the value attached to tokens. Tokens are divided into two types, tokens that relate to something outside of the blockchain, such as immovable property, movable property, personal claims, or other digital assets, and tokens that do not relate to something outside of the blockchain, typically bitcoin. The former tokens are referred to as "non-native tokens" or "exogenous tokens," and the latter are referred to as "native tokens" or "endogenous tokens."[46]

---

44 Financial Market Law Committee (FMLC), "Distributed Ledger Technology and Governing Law: Issues of Legal Uncertainty" (*FMLC*, March 2018), 11–12 <http://fmlc.org/wp-content/uploads/2018/05/dlt_paper.pdf> accessed 28 June 2023.

45 European Banking Authority (EBA), "Report with advice for the European Commission on crypto-assets" (*EBA*, 9 January 2019), 7 <https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2545547/67493daa-85a8-4429-aa91-e9a5ed880684/EBA%20Report%20on%20crypto%20assets.pdf>; HM Treasury, Financial Conduct Authority, and Bank of England, "Cryptoassets Taskforce: final report" (*HM Treasury*, October 2018), 11–14 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf> accessed 28 June 2023.

46 UNIDROIT, "Digital Assets and Private Law Working Group, Fourth Session (Study LXXXII – W.G.4 – Doc. 2) (*UNIDROIT*, October 2021), 74–75 <https://www.unidroit.org/wp

In non-native or exogenous tokens, various assets/values could be connected to blockchains, such immovable property, movable property, personal claims, memberships, other digital assets, *etc.* The extent of the connection between such property, claims, membership, or other assets and the record of the blockchain (whether the title, transfer, or exercise of such property, claim, membership, or other assets is legally linked to and is determined by those of the tokens recorded on the blockchain) should be determined by the governing law of the property, claim, membership, or assets associated with the tokens.[47]

If, according to these laws applied to property, claim, membership, or other assets, the title, transfer, or exercise is to be determined by those of tokens, then title, transfer, or exercise of such assets should be determined by those of tokens. Then, regarding the title, transfer, or exercise of tokens, the law applied to proprietary issues of blockchain should govern (how such law should be determined will be discussed later). On the other hand, if, according to the law applied to property, *etc.*, there is no legal link between title and transfer of the property, *etc.* and the record of the blockchain, then the proprietary aspect should be governed by the law applied to the property under conventional PIL rules.[48] This is the same approach that has been applied to rights for which paper certificates are issued and to rights managed on book entry systems.[49]

-content/uploads/2021/11/Study-82-WG4-Doc.-2-Revised-Issues-Paper-1.pdf> accessed 28 June 2023. The expressions of "native tokens" and "non native tokens" are also used in order to distinguish tokens programmed directly into the architecture as part of the creation of a new blockchain protocol, and tokens issued using the existing blockchain and typically on the second or upper layer (Swiss Federal Council, "Legal framework for distributed ledger technology and blockchain in Switzerland: An overview with a focus on the financial sector" (*The Federal Council*, 14 December 2018), 27, 34 <https://www.newsd.admin.ch/newsd/message/attachments/55153.pdf> accessed 28 June 2023).

47 Swiss Federal Council (n 46) states (i) the law applicable to the underlying contract of the claim is applied to the question to what extent the embodiment of the claim in a token is legally valid and to what extent the transfer of that claim can be linked to the transfer of the token, (ii) the law applicable to the company determines to what extent the embodiment of membership in a token is legally valid and to what extent the transfer thereof can be linked to the transfer of the token, and (iii) the law where property locate determines the extent to which the respective right in rem can be linked to a token. *Id.*, 75.

48 Kozuka (n 8), 23–24. FMLC (n 44) also proposes "where the asset has an existence which is wholly independent of the system—such that the system serves purely as a means of recording the transaction and neither title nor the asset is constituted thereby—the proprietary effects of the transaction should be determined according to the conflicts of rules which would ordinarily apply outside the system."

49 Such approach has been supported by academics in Japan in relation to indirectly held securities. For example, see "Roundtable Discussion: Legal Perspectives on Collateralised Derivative Transactions: In light of Closeout Netting Law" (Japanese: Zadankai: Tanpotsuki Derivative Torihiki womeguru Hoteki Shiza- Ikkatsu Seisan Ho wo fumaete" (1998) 1531 Kinyuhomujijo 11, 28–30 (Comment by Masato Dogauchi); Yoshihisa Hayakawa,

5.3.2 Transactions through Intermediaries

Many transactions related to crypto-assets are conducted through intermediaries such as crypto-asset exchangers. In considering PIL issues related to transactions using blockchains, it is necessary to distinguish between cases in which the rights and obligations of a direct participant in the blockchain are at issue and cases in which the participant participates through an intermediary.[50]

In the former case in which relevant parties directly participate in blockchain and the record of blockchain itself matters, property law issues should be governed by the law applied to property law issues of the blockchain (which will be discussed in 5.3.3). On the other hand, the situation is the same as when the governing law of indirectly held securities becomes an issue in the latter case. There is no statute regarding indirectly held securities in Japan, and it is unclear which law would be applied to property law aspects of indirectly held securities. In the scholarly opinion, the following views are argued; (i) if the global certificate has been issued, the law of the place of the global certificate shall apply, but if the global certificate has not been issued, the law of the claim shall apply;[51] (ii) in the case of a dispute over the ownership of a certificate, the governing law of the location of the global certificate, but in the case of a dispute between parties to a contract, the governing law of the contract shall also be applied to property law issues;[52] and (iii) for indirectly held securities, the governing law of the location where the account is maintained shall be applied.[53] With reference to the Hague Convention on the Law Applicable

---

"Private International Law Issues on Entrusted Assets in Financial Transactions" (Japanese: Kinyutorihiki niokeru Azukari Shisan wo meguru Kokusaisihojo no Mondai," in *Institute for Monetary and Economic Studies, Bank of Japan, Discussion Paper No. 2012-J-11* (*IMES*, 2012), 7–8 <https://www.imes.boj.or.jp/research/papers/japanese/12-J-11.pdf> accessed 28 June 2023.

50 We could distinguish these two cases according to whether a customer manages its secret key himself and has direct control over the asset, or whether he needs an intermediary to exercise control.

51 Zadankai (n 49), 28–30.

52 Kazunori Ishiguro, "Centralised Securities Settlement System and International Insolvency: Focusing on Dematerialised (Paperless) Systems" (Japanese: Syuchuteki Shokenkessai Shisutemu to Kokusai Tosan – Mushoken (paperless) ka ni Juten wo oite," in Kazunori Ishiguro (ed), *Kokusai Kinyu Tosan* (Keizai Houhou Kenkyukai 1995), 384–385. There is one case that applied the governing law of contract to decide a property law issue (if the indirectly held security recorded in an account managed by an intermediary in Japan has been delivered to the customer) (Yamagata District Court Sakata Branch, Judgment on 11 November 1999, Kinyu Shoji Hanrei No. 1098, 45; Sendai High Court Judgment on 4 October 2000, Kinsyu Shoji Hanrei No. 1106, 47).

53 Naohiro Kitasaka, "Governing Law of Rights in Indirectly Held Securities: The 2002 EU Directive, the UCC and the Draft Hague Convention Approach (Japanese: Kansetsu Hoyu

to Indirectly Held Securities, the law of the place where the account is maintained,[54] or when the link between the location of the account and the subject matter is weak, the law agreed upon between the intermediary managing the account and the customer, should be applied to property law aspects. Regarding the property law issues in cases where the participant participates through an intermediary, the same approach should be applied.

5.3.3 Applicable Law to Proprietary Issues of Blockchain

There are views in various countries on how the rule of PIL, which traditionally applies the *lex situs*, should be modified in relation to blockchains. Since the private key plays a vital role in the blockchain, it could be argued that the law of the location of the private key or wallet is the governing law. However, it is not appropriate to focus on the location of the private key or wallet because the private key is just a number and can be easily duplicated and moved, and the location of the private key is often challenging to identify.[55]

For example, the following views are expressed: (i) the system of law chosen by the network participants for the distributed ledger system, which is called 'elective situs' should also govern proprietary effect, and in the case where the elective situs could not be found, the law of the place of the relevant administrator or operating authority (PROMA) or the law of the location of the user should govern;[56] (ii) Relating to proprietary issues among the participants to the system, the law governing the relationship of participants of the system

---

sareta Yukashoken no Kenrikankei no Junkyoho- 2002 nen EU shirei, UCC oyobi Hague Joyaku Soan no Approach nitsuite" (2002) 52 Handai Hogaku 351, 370–372.

54 In a case where the property right of auto vehicles was disputed, the Supreme Court of Japan ruled, "[w]hen a motor vehicle is used in a wide range of operations and its physical location fluctuates, trying to determine the governing law based on the physical location of the vehicle will result in the governing law fluctuating with the movement of the vehicle. In addition, it may be difficult to determine the physical location of the vehicle at a particular point in time. Therefore, the determination of the governing law becomes unstable. In such cases where the relationship between the acquisition or loss of rights in a vehicle and the interests of the country where the vehicle is located is weak, it is more appropriate to use the law of the place where the vehicle is mainly used as the governing law, rather than the law of the place where the vehicle happens to be physically located in the course of its use." It also ruled that the location of the registration of automobiles should be considered as the place where the vehicle is mainly used. Supreme Court Judgment on 29 October 2002, 56 Minshu No. 8, 1964. This case could be used to support the application of the law of the place where the account is maintained.

55 Florence Guillaume, "Aspects of private international law related to blockchain transactions," in Daniel Karus et al. (eds), *Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law* (Elgar 2019), 63.

56 FMLC (n 44), 21–22.

should also govern proprietary issues, while relating to proprietary issues that parties who do not participate in the system concern, the law of the residence or business of the participants who has the closest connection to the issue should govern proprietary issues;[57] (iii) the law chosen by the relevant parties should also govern proprietary effect, but if no such agreement exists, the *lex fori* should govern.[58]

The application of *lex rei sitae* to intangibles is not totally new in Japan. In a case where the law applicable to a pledge of a claim for a bank deposit was disputed, the Supreme Court opined, "Article 10(1) of Horei (Note: the statutes on applicable law when the dispute occurred) stipulates that property rights and other rights to be registered concerning movable and immovable property shall be governed by the law of the location of the subject matter. This is because, in the case of a right such as a property right, which is aimed at the exclusive control of a thing, it is understood that the relevant rights to the object have a close relationship with the interest of the location of the object. Although the pledge of right is a property right, it is impossible to directly inquire about the location of the object because the object is a claim itself and not tangible. On the other hand, since a pledge of a claim governs the subject matter of the claim and directly affects its fate, it is reasonable to conclude that the law applicable to it should be the law governing the subject matter of the claim itself." According to this Supreme Court judgment, under Japanese PIL, it should be said that when it is impossible to find the location that has a close relationship with the subject matter, the property law aspects should be governed by the law that has a close relationship to the fate of the subject matter.

The basic principles/policies of connecting factors should be (i) objective and easily ascertainable, (ii) has better control over the asset, and (iii) reasonably reflect the reality of the systems as far as possible.[59] Considering the different types of asset holdings and DLT systems, no single rule could cover every situation, and some waterfall framework (A framework of presenting several rules in a prioritised order, rather than setting down to one rule, and proceeding to the next ranked rule unless a higher priority rule applies) by which the most appropriate governing laws could be determined depending on their types should be considered.

---

57 Andrew Dickinson, "Cryptocurrencies and the Conflict of Laws," in David Fox and Sarah Green (eds), *Cryptocurrencies in Public and Private Law* (Oxford: Oxford University Press 2019), 126–137.

58 Guillaume (n 55), 78–81.

59 (i) and (ii) are considered as the rationale for the application of the *lex situs* to many questions of property law (Lord Collins of Mapesbury and Jonathan Harris (eds), *Dicey, Morris & Collins on the Conflict of Laws* (15th edn, Sweet & Maxwell 2018), 1295).

First, as supported by the views introduced earlier, where the participants in the blockchain choose the governing law, that law should govern the property law issues. This includes not only the case where parties agree on the applicable law to property law issues but also the case where parties agree to the applicable law to contract issues. In the latter case, the coverage of the governing law of contract should be extended to property law issues, unless parties have expressly agreed otherwise. Considering the nature of distributed ledgers, where transactions take place over the Internet, and multiple nodes record the same information, and it is difficult to objectively determine the most closely related ground, such an approach should be considered reasonable. Especially in a permissioned blockchain, where not everyone can participate, there seems to be a good reason that those who are permitted to participate in the system are allowed to agree on the governing law that applies to their system:[60] it would contribute to the stability of legal relations.[61] With respect to the application of the law agreed to by the participants in the system as the law governing property rights in relation to third parties who do not participate in the system, the above mentioned Japanese Supreme Court precedent on the applicable law on a pledge of a claim has already admitted that the law chosen by the parties could be used as the law governing property rights even in relation to third parties.[62]

However, at least concerning the distributed ledger, which plays an important public role, such as an essential system in the financial market, it is not appropriate to allow completely free choice of governing law in order to ensure that the blockchain is under a proper legal order. In such a case, a choice of law should be subject to regulators' approval.

Even in cases where there is no choice of governing law by the parties, if it is clear that there is an administrator who plays a central role, such as having a certain authority in the system, it may be appropriate to use the location of the administrator as the connecting factor.[63] This is because if there is an administrator known to the participants, using the administrator's location as the connecting factor seems to be appropriate to provide clarity and predictability.

60 However, even in a permissionless system, agreement on applicable law may be found as discussed above in relation to the applicable law of contract.

61 Kozuka (n 8), 20.

62 As for the concern that the law agreed upon by the participants in the system is binding on third parties, it has been pointed out that this is the same as being bound by the governing law of the claim when attempting to take a claim as collateral (Michael Ng, "Choice of law for property issues regarding Bitcoin under English law" (2019) 15 Journal of Private International Law 315, 333).

63 This is the approach that FMLC (n 44) proposed.

Also, it would be expected that the location of such a key player might have better control over the blockchain or asset than other locations.

However, it is difficult to determine what level or role is sufficient for an administrator here. Since the basic idea of distributed ledger is to allow participants to transact with each other securely without such an administrator, it would not be easy to find an appropriate administrator to serve as a connecting factor. A key player here should have the power to administer/control the system to some extent because one of the rationales of this connecting factor is control over the system. Simple miners in Bitcoin, therefore, do not qualify. Where there are two or more players with similarly significant powers, we should decide which location is more closely related to the system by considering all circumstances.

If neither of the above two linkages can be found (for example, in the case of Bitcoin, neither party's choice nor a specific administrator can be found), then the law of the location of the person holding the asset or token in dispute (which is likely to be the same as the location of the defendant), or, in the case of a person who holds assets or tokens through an intermediary, the law of the location of that intermediary should govern.

This is because, in situations where the title to or transfer of a particular asset or token on the blockchain is in dispute (and it is in such cases that the governing law for property law issues needs to be determined), it seems that the law that is most closely connected to the person who actually has the power to dispose or transfer the asset or token by making a necessary change of record, should be used as the connecting factor. Given that most legal disputes occur between persons who actually exist (although this assumption may change in the future as technology develops), even if the transaction takes place on the internet, there is good reason to focus on the location of the person who can actually dispose of or transfer the assets or tokens, and it would contribute more effective resolution of disputes in a real world. If the law of the location of the person who is currently in possession of the asset or token, or the law of the location of the intermediary who is managing them, recognises that the asset or token belongs to the plaintiff rather than the person who is currently holding them, it would be easier to obtain a judgment ordering the person to return the asset or token or to enforce such a judgment. On the other hand, if, according to those laws, the person who currently holds such assets or tokens is considered to have legitimate authority, it would not seem easy to obtain effective relief.[64]

64 Kozuka (n 8) agrees with the waterflow framework as proposed in this article and proposes the application of the *lex fori* as a final backstop. *Id.*, 22–23.

Finally, for example, suppose A and B enter into a contract for the sale of crypto-assets recorded on the blockchain. When a dispute about the ownership of the assets occurs, applying the law governing the contract between A and B also to the issue of ownership seems to be more natural because the law has the closest relationship to the dispute.

6 Conclusion

In order for DLT to be used safely in our society, it is necessary that the rule of law is applied, disputes can be resolved through an effective dispute resolution system, and the necessary regulations are applied from the perspective of user protection and social system stability. If the distributed ledger becomes a legal vacuum, it will not be possible to use it with confidence.

Considering that the transactions on the blockchain are conducted cross-border, significant differences in the content of laws of countries could impede the safety and smoothness of transactions.[65] As far as possible, international harmonization should be aimed at also for the rules of PIL.

65 Matthias Lehmann, "National Blockchain Laws as a Threat to Capital Markets Integration" (2021) 26 Uniform Law Review 148, 167–170.

Index

access to justice 55o, 586, 587, 612, 621–623, 631*n*271, 632
applicable law 3, 4, 6, 7, 1o, 14–16, 18, 2o, 24, 26, 27, 35, 41, 43, 45, 51, 6o, 62, 65, 78, 79, 88, 9o, 92, 94, 1o1*n*1, 1o7, 112, 114, 116, 122, 123, 126, 128, 135, 144, 145, 148, 149, 151, 153, 158, 166, 169, 172, 176, 177, 18o, 181, 184–186, 188, 191–194, 196, 197, 2oo, 2o5, 2o6, 2o8, 222, 23o, 247*n*1o4, 256, 26o, 271, 275*n*79, 275–278, 28o, 282, 283, 287, 289, 29o, 298, 31o, 311, 318, 335, 338, 34o, 342, 344, 346, 347, 351, 362, 387*n*67, 388, 39o, 392, 393, 395, 4o1, 413, 415, 416, 447, 449, 45o, 453, 455, 464, 468, 47o, 473, 483, 485–489, 491, 494, 496, 5o1, 518, 52o*n*8o, 526, 549, 552, 583*n*116, 587*n*129, 592, 595, 661, 674, 686, 687, 69o, 694, 7oo–7o7, 7o9*n*1, 727, 732, 735*n*43, 739*n*64, 74o, 741, 743, 746, 75o, 753, 757, 758, 76o, 761, 766, 77o, 779, 78o, 785–787
arbitration 7, 29, 222, 371, 386*n*61, 44o, 48o, 532, 57*1n*86, 588*n*13o, 592–6oo, 6o2, 6o3, 6o5*n*186, 6o9–611, 612*n*2o3, 614*n*2o8, 614, 616*n*217, 616*n*219, 617, 631, 633–635, 636*n*287, 637*n*29o, 64o, 642, 643, 644*n*6, 649, 65o, 652–665, 667, 668, 676, 714, 727
asset tokenisation 3o–32, 287, 29o, 291, 294, 299, 3oo, 3o7, 3o8, 312, 313

bills of lading 62, 336*n*96, 494–497, 497*n*6, 498–5o1, 5o5, 5o8, 5o9, 513*n*58, 514*n*59, 515, 517*n*69, 517*n*71, 518, 519*n*78, 764
bitcoin 1, 3, 4*n*5, 12*n*5, 13*n*13, 14*n*16, 36, 39*n*118, 52*n*4, 53, 54, 56, 58*n*3o, 59–61, 67–7o, 72, 76, 78, 79, 81, 82, 85–87, 89, 9o*n*29, 91–1o1, 1o5, 1o6, 1o7*n*19, 119, 123*n*55, 124, 125, 127, 135*n*17, 135*n*18, 139, 152*n*67, 163*n*32, 173*n*6o, 183*n*96, 193, 214, 215, 219, 22o, 229, 23o, 231, 233*n*72, 245*n*99, 246, 259, 261, 262, 264, 265, 266*n*35, 267*n*44, 268, 271, 275*n*8o, 279*n*94, 288*n*14, 292*n*29, 294, 297, 298*n*62, 3o1, 314, 315*n*5, 317*n*16, 321*n*33, 321*n*34, 322, 324, 326, 327, 33o–334, 336*n*97, 341, 343*n*127, 344*n*131, 352*n*1o, 356*n*26, 357*n*29, 372, 378, 379, 39o*n*83, 395*n*98, 396, 399*n*2, 399*n*4, 4oo*n*6, 4o1, 4o4*n*28, 411*n*72, 411*n*77, 419–422, 423*n*18, 423*n*19, 427, 43o, 436–438, 44o–442, 443*n*7o, 443*n*71, 443*n*72, 449, 457, 458, 46o, 464, 475*n*43, 48o*n*3, 48o*n*4, 529, 537, 538, 539*n*19, 542, 544, 551, 554, 558*n*33, 6o1*n*177, 625*n*245, 629*n*264, 638, 639, 643–648, 662, 663, 666*n*45, 674, 675*n*9, 677*n*21, 681, 682, 686*n*97, 69o*n*126, 691*n*136, 7o6, 713*n*12, 716, 72o, 744*n*89, 751*n*129, 759, 765, 766, 782, 787*n*62, 788
Blockchain Dispute Resolution (BDR) 8, 42*n*141, 481*n*5, 549, 55o, 57*1n*86, 6o2–64o, 656
blockchain layers 63, 291, 298, 3o3, 3o7, 512, 526, 554*n*17, 68o, 783*n*46
See also blockchain architecture 63, 5o9
blockchain transactions, 7, 8, 1o1*n*1, 32o, 381*n*46, 4o7*n*47, 586*n*127, 624, 69o, 751, 757*n*2o, 779, 785*n*55
bond(s) 1o9, 144*n*2, 161, 212, 245*n*1oo, 281, 285, 295*n*38, 3o2*n*83, 377, 382, 383, 394, 42o, 457, 492, 5o1, 5o3, 51o, 515, 52o*n*8o, 521*n*88, 687, 696, 738, 739, 747
Brussels I Bis Regulation 77*n*51, 88, 89, 92–94, 666
Brussels I Recast Regulation 217, 219, 221*n*47, 223*n*51, 223*n*53, 225, 226, 229, 23o, 242*n*94, 243, 245, 249, 257

central bank(s) 6, 36, 37*n*1o4, 37*n*1o6, 37*n*1o7, 38, 71, 72, 99, 1o5, 115, 116, 2o4, 262*n*16, 264, 265, 267, 268, 29o, 315*n*7, 316*n*11, 317, 318*n*18, 318*n*21, 322*n*41, 344*n*131, 351–353, 354*n*15, 354*n*16, 355, 356, 357*n*27, 357*n*3o, 358, 359, 361, 366–369, 371, 376*n*18, 417, 42o, 424–428, 429*n*36, 431, 432, 456, 51o*n*5o, 642, 644, 7o7, 715

characterisation 5, 6, 15, 31, 33, 34, 37, 40, 41, 45, 92, 96, 98, 99, 140, 157, 158, 166–171, 177, 189, 193, 194, 196, 197, 199, 201–205, 208, 209, 216–221, 231, 232, 244, 254, 256, 257, 260, 266, 269, 270*n*60, 276, 284, 294, 297*n*59, 304, 318, 320, 324, 342*n*118, 385, 389, 400, 403, 404, 452, 479, 481, 486, 487, 493, 488, 584*n*120, 739, 754
choice of law 3–5, 10, 14, 15, 18, 192*n*30, 20, 22, 27, 38, 39, 43, 101, 122, 123, 127, 147–149, 150, 151, 158*n*4, 200*n*158, 205, 210*n*4, 211, 212*n*13, 212*n*15, 213, 217, 223, 224, 238, 239, 240, 242, 247, 249, 251*n*108, 251*n*109, 251*n*110, 253*n*115, 260, 264–267, 268*n*49, 268*n*50, 271–278, 279*n*94, 281, 283, 284, 292, 295, 300, 301*n*74, 303, 310–313, 336*n*97, 339, 340*n*114, 343, 345, 346*n*135, 363, 371, 386, 387, 390, 392, 393, 394, 396, 397, 398, 411*n*72, 414, 415*n*103, 454, 461, 466, 467, 469*n*30, 469*n*32, 470, 471, 488, 494, 496, 504–508, 512, 515, 516*n*65, 518, 520, 521*n*85, 521–528, 543, 544, 596*n*161, 686, 694, 699, 700, 704, 706, 708, 709, 711, 744, 745, 752, 757–760, 762–764, 779, 787
claim(s) 17, 22, 24, 36, 45, 60, 61, 73, 79, 88, 92–94, 106, 108, 110, 111, 116, 120–122, 125, 138, 140, 144, 162, 163, 171*n*55, 174–176, 188–191, 193, 194, 197, 199, 201, 202, 207, 209, 210, 212*n*13, 213, 216–218, 222, 224, 227, 228, 230–232, 234–237, 241–245, 247–250, 256, 257, 274, 282, 283, 288*n*17, 293, 294*n*35, 297, 310, 323, 327, 328, 330, 335, 336, 337*n*100, 338, 341, 342, 352, 355, 368, 371, 379, 380, 388, 394, 395, 397, 398, 402–404, 407*n*46, 411, 413, 425, 435, 437–439, 440–442, 445–447, 450, 452–455, 459, 460, 463, 470*n*34, 472, 474, 494, 496, 499, 504*n*32, 505, 515, 527, 532, 587, 596*n*159, 619, 625, 654, 674, 684–687, 694–703, 705, 732, 748, 756*n*11, 759, 761–763, 766, 767, 780, 782–784, 786, 787
conflict of laws rules 2*n*2, 14, 31*n*76, 42, 81*n*2, 101, 106, 108, 109, 165–167, 168*n*45, 168*n*47, 169–171, 172*n*56, 173–176, 178, 180, 188, 190, 192, 194, 196–200, 201*n*161, 202, 203, 209*n*3, 210*n*4, 212*n*13, 212*n*15, 214, 218, 239, 240, 251*n*108, 251*n*109, 251*n*110, 253*n*115, 254, 255, 268*n*47, 268*n*49, 270*n*59, 282*n*104, 282*n*108, 298*n*63, 301*n*74, 304*n*90, 313, 315, 327*n*52, 334*n*83, 340*n*114, 340*n*115, 343, 346*n*135, 347*n*136, 352, 353, 374, 386, 387, 394, 399*n*3, 402, 414*n*94, 462, 468, 471, 476*n*46, 486, 514*n*59, 516*n*65, 520*n*82, 529, 543, 549, 673, 686, 706, 709, 746*n*102, 757–759, 786*n*57, 786*n*59
connecting factor(s) 3, 6, 7, 9, 14–25, 26*n*51, 27, 31*n*77, 35, 45, 51, 58–60, 62, 63, 65, 78, 88, 96, 101, 109, 113–115, 121–127, 146, 149, 150, 158, 165, 168, 180, 182, 196–200, 208, 211, 212, 214–218, 220, 231, 250–252, 254*n*124, 255, 256*n*130, 257, 260, 264, 267, 268, 271, 276–279, 281–284, 289, 292, 293*n*32, 300–306, 309, 310, 312, 313, 318–330, 335, 336, 338, 340, 346, 347, 353*n*12, 385, 389, 390, 392, 393, 395, 397–399, 406, 408, 412, 413, 416, 449, 454, 465, 467, 471–473, 485–489, 491, 493, 506–508, 521, 525, 549, 560, 561, 569, 570, 572, 574, 577, 578, 580, 585, 602, 623, 727, 734, 735, 739, 740*n*65, 740*n*67, 740*n*68, 741, 743–754, 757–759, 761–763, 782, 786–788
consensus mechanism(s) 51, 54–57, 63*n*44, 70, 75, 105, 296*n*62, 354*n*14, 380*n*35, 402, 410, 421, 615
crypto asset(s) 6, 7, 12*n*9, 14, 15*n*20, 16*n*22, 26, 27, 39, 45, 56–58, 66–70, 71*n*26, 72*n*28, 73–76, 78–80, 91, 94, 100–102, 104–108, 110, 111, 115, 116, 118, 119, 122, 123, 125–128, 131, 133, 135–139, 141–148, 151, 152, 157–160, 161*n*17, 164–174, 178–208, 213–229, 231–234, 236–238, 242–246, 248–250, 255–257, 259–280, 282, 284, 290*n*24, 295, 297, 314*n*3, 315, 319, 320, 321*n*34, 322, 323, 327–331, 336–338, 340*n*112, 341*n*117, 342, 343*n*127, 345–347, 357, 372, 374, 376*n*20, 378, 383, 389*n*80, 395, 399, 400, 401, 403, 404, 406, 408, 409, 414–416, 421*n*14, 426, 431–450, 451–455, 486, 491, 496*n*5, 500*n*17, 502*n*28, 504*n*32, 511, 523*n*97, 537–539, 544, 549, 553, 556, 582, 588, 589, 591, 602, 605, 607–609, 612, 613, 617, 623, 625, 632, 633, 638, 648, 655, 677*n*19, 745*n*92, 754, 766, 767, 769, 774, 776, 777*n*30, 778, 781, 782*n*45, 784

crypto economy 549, 550, 555, 556, 563, 612, 613, 621–623, 625, 626, 628, 630, 632, 639
See also crypto economic 553, 556, 613, 615, 621, 628, 630, 632, 640
cryptography 12, 36, 51, 52, 57, 65, 71, 84, 104, 130, 160, 165, 261*n*7, 262, 314*n*2, 331*n*73, 442, 490*n*36, 666*n*45, 675, 696, 706
See also cryptographically 12, 32, 67, 74, 89, 93, 94, 104, 215, 233*n*72, 273, 287, 292, 316, 317, 319, 326, 327, 332, 431, 444, 446*n*80, 456, 629, 675, 782
crypto securities 109, 117, 161*n*17, 466*n*21, 495, 501, 502, 504, 505, 507, 508, 510–512, 515, 516, 522–527, 730, 731, 738
custody 31, 34*n*90, 37, 60, 77, 109, 117–119, 122, 125, 136*n*22, 221, 233, 237, 307, 308, 323*n*41, 433*n*45, 443–445, 446*n*80, 454, 465–468, 471, 473, 478, 501, 539, 542, 544, 694, 738

decentralisation 133, 142, 319, 389, 448*n*90, 449, 633, 640, 629*n*264
decentralised finance (DeFi) 40, 71*n*25, 141, 142, 143*n*36, 144, 148–152, 157, 287, 289, 373*n*8, 446, 447, 452, 458, 459, 465, 472, 510, 511, 550, 552*n*8, 555, 556, 589*n*135, 612, 639, 640, 675*n*5, 680, 716, 717
Decentralized Autonomous Organization (DAO) 1, 6–8, 30, 35, 40, 42, 43, 64, 65, 78, 86, 152, 178, 288, 303, 308*n*99, 396, 402, 448, 450, 481, 482, 550–577, 579–592, 602, 603, 605, 607, 610–613, 615*n*216, 616, 618–621, 623–625, 633, 635, 639, 640, 677, 678*n*24, 680*n*45, 718*n*24, 746*n*99
decentralized justice 608*n*195, 612*n*203, 629
derivatives transactions 529, 530, 533, 535, 536, 541, 543
dispute resolution 1, 7, 8, 28, 291*n*65, 41*n*133, 42*n*141, 47, 221–223, 234, 468, 481*n*5, 549, 550, 555, 570, 571*n*86, 586, 591, 592, 595*n*157, 596, 597, 598*n*168, 598*n*169, 599, 600*n*171, 600*n*172, 600*n*173, 601, 603–613, 614*n*208, 614*n*209, 615–621, 622*n*233, 623, 625–627, 628*n*252, 629*n*261, 630–634, 636*n*287, 639, 642–666, 668, 669, 676*n*16, 751, 770, 789

elective situs 6, 18–20, 24, 110, 123, 127, 292, 301–303, 312, 345–347, 543, 544, 785
electronic securities 70, 109, 117, 119, 126, 198*n*152, 382, 383*n*52, 464*n*18, 503, 504, 507, 508*n*48, 513*n*57, 729, 737*n*54, 739*n*63, 742
extraterritorial 250*n*106, 354, 365*n*67, 367*n*78, 368, 370, 711, 722, 766, 767, 772, 774–777

fair justice 621, 626, 628, 630, 638, 640
financial instrument(s) 30, 68, 79, 92*n*34, 111, 112, 116–119, 122, 148, 150, 161, 162, 184–187, 202*n*166, 239, 264, 274, 277, 280, 281, 295*n*38, 296, 322, 329, 342, 357*n*27, 394*n*94, 432*n*42, 432–436, 483, 504*n*32, 543*n*28, 648, 678, 696, 753, 774
forum loci rei sitae 209
fraud 32, 33*n*85, 73, 90*n*29, 226, 227, 229–231, 310, 315*n*4, 321*n*34, 324, 331, 399, 401, 404*n*31, 456, 461, 469, 470, 476, 480, 644, 712*n*9, 713, 717, 719, 722*n*41, 723*n*41, 773, 774
See also fraudulently 85, 230, 314*n*4, 403, 714

German 7, 43*n*146, 68, 70, 109*n*26, 117, 146*n*46, 193*n*129, 197*n*142, 198, 201*n*162, 201*n*163, 218, 219, 269*n*52, 281, 282*n*108, 296, 322, 365*n*65, 376*n*19, 381–384, 389*n*79, 389*n*80, 396, 405*n*42, 412*n*84, 423, 453*n*107, 463*n*17, 464*n*18, 494, 497, 501, 503, 504, 507, 513*n*57, 514*n*59, 515*n*62, 520*n*81, 531, 694, 701, 709*n*1, 712*n*9, 727, 729, 730, 732–734, 736–746, 752, 753
See also Germany 8, 43, 78, 109, 116, 117, 119, 185*n*101, 211*n*8, 219, 269*n*52, 396, 510*n*53, 709*n*1, 727, 728, 730*n*17, 733, 734, 739–742, 744–746, 749*n*123, 751, 752, 754
global standards 44, 374*n*12
governance 30*n*74, 35, 44, 47, 48, 63, 75, 81*n*2, 141, 152, 185*n*101, 213*n*20, 215*n*30, 303, 308*n*99, 319*n*24, 421*n*16, 448, 476*n*48, 481, 485, 525, 550, 552–554, 555*n*23, 558*n*30, 559–563, 565, 569, 571–579, 582, 588, 591, 602, 607, 608, 610–613, 619–621, 623, 624, 632, 639, 650*n*18, 731*n*24, 751*n*132

insolvency 6, 13*n*9, 27, 32, 37, 44–46, 53*n*7, 125, 205–207, 274–276, 291, 322*n*37, 344, 382, 388, 396, 417, 421, 432, 437*n*52, 438–442, 444–448, 450–455, 461, 465*n*19, 474, 477, 538, 539, 541, 542, 691, 692, 729, 784*n*52
intangible asset(s) 17, 24, 122, 212, 213, 242, 243, 250, 256, 258, 292, 293*n*35, 297, 325, 335, 339*n*107, 390, 463, 472, 521, 686
intellectual property 13*n*9, 14, 33, 34, 45, 46, 93*n*42, 101, 193, 194, 197*n*145, 197*n*146, 198, 236, 239, 240, 242, 243, 247, 270, 282, 297, 299, 300, 390, 414*n*93, 414*n*94, 706, 711
investment securities 336*n*96, 494, 495, 500, 501, 515, 520

Japan 8, 57, 74, 185*n*101, 314*n*4, 351*n*2, 376*n*20, 441, 502, 517, 519*n*78, 767–778, 779*n*36, 781, 783*n*49, 784, 785*n*54, 786
See also Japanese 53*n*7, 54*n*10, 61, 90*n*29, 318, 376*n*20, 388*n*75, 420, 423*n*18, 441, 460, 494, 497, 500*n*16, 518*n*75, 520*n*80, 765, 767–774, 775*n*25, 775*n*26, 776–778, 779*n*36, 779*n*37, 780*n*39, 781, 783*n*49, 784*n*49, 784*n*52, 784*n*53, 787
jurisdiction 7, 8*n*7, 10, 11, 13–15, 17, 18, 21, 24, 28, 29, 32, 37, 41–44, 45*n*160, 47, 68, 71, 74, 77*n*51, 78, 80, 88–94, 100, 101*n*1, 110, 112, 114, 128, 136, 138, 144–146, 151, 172, 174, 176, 177, 190, 192*n*120, 194, 199, 202, 205, 208–212, 217–227, 230, 234–236, 237*n*85, 238, 243–245, 246*n*102, 247, 249, 250, 255, 256*n*131, 257, 266, 267, 269, 270, 272, 278, 280, 282, 283, 289*n*22, 293, 295, 297, 298*n*61, 298*n*64, 299, 302, 304, 306, 310, 315*n*4, 320–322, 336*n*95, 340*n*112, 341*n*117, 351*n*2, 354*n*16, 365*n*67, 367, 371, 383–385, 397, 404*n*28, 406, 407*n*46, 407*n*50, 412, 414*n*94, 414*n*95, 447–452, 454, 455, 460–462, 467, 468, 472, 484, 486, 500, 513*n*58, 523, 524*n*102, 525, 531–535, 538, 542–544, 549, 550, 554, 556–558, 561–565, 568–570, 572–590, 591*n*142, 592, 596, 602, 605, 608–612, 617, 619–621, 624, 626, 630, 633–635, 638–641, 653*n*26, 666*n*46, 667, 668, 673, 686, 687, 690, 708, 710–713, 718*n*24, 719, 721, 722, 723*n*41, 723*n*42, 754, 755, 758, 760, 762, 766–772, 775, 777, 780

ledger-based securities 325, 379, 380, 498, 499, 501*n*23, 503, 506, 685, 695, 696, 700, 757*n*17
lex cryptographia 4, 39, 67, 84–87, 320*n*28, 400, 414, 415, 751
lex loci delicti 400, 405, 408, 410, 412
lex situs 16*n*22, 17, 23, 25, 120, 121, 209, 211, 212, 216, 238, 244, 249, 251–254, 257, 271, 277, 292, 299, 300, 304, 305, 335, 337, 343*n*127, 488, 518, 519*n*78, 781, 785, 786*n*59
Liechtenstein 7, 8, 43*n*149, 44*n*153, 74, 75*n*40, 108, 120, 124, 198, 293*n*35, 296, 308, 309, 379*n*31, 380, 381, 384, 390*n*86, 391, 502, 503*n*29, 504, 510*n*51, 748*n*115, 754–759, 761–764

nodes 1, 11–13, 16, 28, 51, 54–57, 59, 73, 105, 131, 146, 152*n*67, 173, 175, 213, 215, 262, 263, 288, 337, 345, 353, 389, 402, 411, 442, 443, 458, 459, 462, 463, 471, 491, 529, 551, 586, 625, 675, 723*n*42, 753, 767, 771, 773, 774, 781, 787
Non-Fungible Tokens (NFTs) 30, 32–34, 40, 45, 61, 62*n*40, 62*n*42, 105, 119, 148, 151, 285, 286, 289, 292, 297, 303*n*89, 307, 401, 567, 582, 591, 647, 648, 655, 677, 680, 681, 689, 723, 765

off-chain enforcement 42, 550, 621, 633, 635, 636, 638
on-chain 8, 24*n*43, 25, 26, 31, 32, 73, 76, 134, 135, 138–140, 146, 148, 150, 338, 482, 483, 490, 491, 518, 561, 578, 581, 582, 590, 602, 604, 607, 609, 611–613, 615, 617, 618, 622, 623, 633, 634, 640, 641, 653, 654, 668, 669, 677, 678
Online Dispute Resolution (ODR) 549, 550, 571*n*86, 591, 592, 595*n*157, 596–609, 612*n*203, 613, 614, 616, 618, 621–623, 627–629, 630*n*271, 634, 636, 639, 644*n*6, 645*n*9, 649, 650, 651*n*19, 652*n*25
overriding mandatory rules 19*n*30, 101, 205, 334, 370, 479, 491–493, 533, 758

party autonomy 3, 4, 7, 11, 15, 18, 19*n*30, 20, 26, 27, 38, 39, 60, 210*n*4, 260, 277, 278, 309, 340, 347, 363*n*56, 386, 392, 395, 397, 400, 414, 461, 466, 468–470, 486, 585, 735, 744*n*87, 752, 757, 759
personal data 132, 171*n*55, 194, 195, 367, 369, 371, 404*n*27, 645
private justice 330, 550, 555, 592, 601–603, 609, 621, 626, 630, 631, 634, 640
property 4*n*5, 5, 6, 13*n*9, 14, 17, 33, 34, 36, 37, 39, 44–46, 65, 66, 91, 93*n*42, 100, 101, 104–106, 108, 109, 113, 115, 117, 121, 123, 145, 159, 164*n*34, 171, 180, 188, 189, 193, 194, 197–202, 205, 206, 209, 210*n*4, 211–214, 216, 220, 222, 229, 230*n*64, 233, 235–245, 247–252, 253*n*115, 255–258, 260, 266, 269, 270, 271, 274, 276, 279*n*94, 282–284, 286, 289*n*18, 292*n*31, 293, 297–300, 301*n*74, 303–305, 308, 311, 320, 321*n*34, 322, 323*n*43, 324*n*43, 324*n*45, 330*n*69, 331, 332, 335–340, 343, 344, 346, 352, 380–386, 388–390, 392–394, 397, 398, 411*n*72, 414*n*93, 414*n*94, 436–442, 445, 446, 448, 452, 453, 468, 469*n*32, 470*n*34, 474, 488, 501*n*21, 518, 519, 537–539, 582, 600, 607, 634, 655, 685, 693, 706, 710, 711, 717, 718*n*24, 722*n*41, 756*n*11, 758, 759, 762, 763, 764*n*61, 767, 768, 772, 773*n*21, 774*n*23, 780–788
proprietary claim(s) 61, 216, 230–232, 237, 241, 244, 245, 250, 252, 256, 439
proprietary rights 34, 101, 104, 107, 111, 114–116, 120, 121, 125, 126, 196*n*141, 209*n*2, 246, 256, 277, 282, 289, 291, 296, 308, 333, 344, 392, 460–462, 464–466, 469, 470, 519*n*78, 538
pseudonymity 3, 7, 13, 16, 39, 42, 54, 87, 89, 90, 93, 94, 128–133, 138, 140, 141, 143, 144, 147, 149–153, 399, 488, 549, 550, 553, 557, 559, 575, 577, 585–587, 589, 591, 602, 604, 607, 640, 769

recognition and enforcement 8, 10, 14, 28, 29, 32, 33, 37, 42, 77*n*51, 88*n*18, 92*n*37, 114, 145, 172*n*57, 205*n*183, 221*n*47, 407*n*50, 532, 534*n*8, 572, 593, 594, 599, 633, 636, 637, 642, 643, 646, 648, 649, 652, 654–656, 658, 659, 661–669, 709, 710, 714*n*14
renvoi 310–312, 734, 735*n*43, 742, 743, 751
rights in rem 109, 126, 206, 209, 244, 297*n*56, 382, 392, 393, 453, 474, 678, 684, 685, 687, 693, 698, 699, 701, 708, 729, 730, 733, 734, 746, 761, 762
Rome I Regulation 19*n*30, 87, 88, 89*n*23, 90, 92, 94, 101, 120, 147–150, 165*n*41, 166*n*41, 166*n*42, 169, 170*n*54, 171*n*55, 172, 174–191, 196, 204, 205*n*181, 217, 226, 247, 248, 253*n*118, 272, 280, 281, 296*n*49, 301*n*72, 346, 353*n*12, 363*n*56, 363*n*57, 364, 387, 395, 403*n*21, 403*n*23, 468*n*29, 487, 489, 491, 514, 515*n*63, 521*n*85, 532, 533*n*6, 740*n*69, 744*n*85
Rome II Regulation 88*n*19, 92*n*39, 144–147, 148*n*52, 169, 170*n*54, 172, 175, 176, 177*n*75, 190–194, 196, 204, 217, 227*n*57, 228, 229, 247, 248, 334*n*83, 403*n*21, 403*n*23, 404, 405*n*35, 405*n*41, 406, 408*n*54, 409*n*62, 410, 411*n*73, 412*n*84, 413*n*86, 413*n*88, 413*n*92, 414*n*96, 414*n*98, 415*n*106, 745, 751

secured transactions 6, 26*n*51, 34*n*90, 122, 259*n*2, 300, 456–459, 461–465, 468–478, 515*n*64, 521, 542, 544, 718*n*24
security tokens 28*n*63, 67, 70, 72, 77, 78, 106, 137, 144, 150, 162, 264, 265, 286, 292*n*29, 294, 295, 306*n*96, 388*n*70, 458, 501, 502*n*27, 511, 524*n*102, 756*n*16, 782
service out of the jurisdiction 210*n*5, 224, 230, 231, 238
smart contract(s) 1, 5–7, 10, 12*n*5, 14, 28–31, 34, 37, 63, 64, 68, 70, 73, 78, 79*n*60, 81*n*2, 123*n*55, 129, 134*n*16, 140–142, 148, 151, 164, 191, 192, 195, 214*n*23, 246*n*102, 263*n*19, 270, 274*n*77, 288, 292, 298*n*64, 310, 316, 319, 320*n*33, 353, 378, 383*n*53, 404*n*32, 407*n*47, 422*n*16, 438*n*54, 479–493, 502, 512, 529–531, 538–540, 549, 551–555, 562*n*47, 564–566, 569–572, 579, 580, 581, 582*n*112, 583–586, 588–591, 602–604, 606–613, 616–619, 622–624, 631*n*274, 632–635, 639, 640, 647–649, 652*n*25, 654, 676*n*16, 679, 680, 690, 713, 716, 744, 751*n*132, 769*n*8, 770, 779*n*37, 785*n*55

stablecoin(s) 3, 36, 38, 39, 67, 70*n*22, 106, 119, 152, 262, 265, 268, 290, 318, 327, 357, 358, 372–398, 421, 431–434, 436, 458, 678*n*31, 716*n*22
stock(s) 245*n*100, 380, 420, 502*n*26, 712, 716, 724, 760
Switzerland 5, 8, 43*n*149, 44*n*153, 51*n*1, 53*n*8, 59*n*36, 74, 108, 117, 129, 135, 136, 145*n*38, 305*n*94, 327*n*54, 379, 384, 385, 387, 395, 443*n*72, 498, 499, 503–505, 511*n*55, 518*n*76, 521, 526*n*107, 552*n*10, 553*n*14, 559–562, 568, 573, 574, 576, 580, 582, 584, 585, 586*n*125, 593, 659*n*37, 673, 678, 687–689, 691, 693, 707, 754, 756*n*16, 761*n*44, 761*n*45, 764, 783*n*46
See also Swiss 31*n*76, 59*n*36, 72, 74, 76, 97, 108, 114, 129, 135–137, 138*n*26, 162*n*28, 230, 265, 268*n*47, 296, 311, 312, 321*n*34, 325–327, 351*n*2, 360, 363*n*56, 363*n*57, 365*n*65, 365*n*68, 372*n*4, 374*n*12, 379, 380, 387, 390*n*83, 395*n*96, 397, 405*n*41, 410*n*67, 411*n*73, 446, 463*n*17, 469*n*30, 492–494, 498, 501, 503, 505, 511*n*55, 513*n*57, 513*n*58, 515*n*62, 519*n*78, 520*n*81, 522*n*90, 551*n*2, 552*n*8, 558–560, 561*n*43, 562*n*44, 562*n*47, 568, 572–574, 576, 580, 582–584, 586*n*125, 593, 673, 674, 676, 677, 678*n*24, 680*n*46, 682, 684–687, 688*n*108, 689–692, 693*n*147, 693*n*148, 696, 702, 707, 756*n*13, 757*n*17, 759*n*33, 762*n*52, 763, 764*n*61, 764*n*62, 783*n*46, 783*n*47

taxonomy 5, 15*n*20, 76, 130, 157–160, 164*n*40, 165–168, 207, 213, 242, 243, 274, 388*n*70, 674, 676, 677, 682, 683
technology neutrality 66*n*2, 72, 73, 75, 79, 166, 353, 500, 503
title transfer 293, 462, 535, 540, 541
tokenisation 30–32, 35, 71, 106, 120, 121, 163*n*33, 285–288, 289*n*18, 289*n*20, 290, 291, 293, 294, 297, 299, 300, 305, 307, 308, 312, 313, 377, 510*n*53, 679, 702, 756*n*16
tokenised securities 501, 754
tokens 1, 5, 7, 8, 14*n*14, 15, 17, 24, 25, 30–32, 35, 38, 48, 50, 61, 62, 67, 69–72, 75*n*40, 75*n*41, 77–79, 104–106, 108, 110, 114, 116, 117, 119, 120, 122–124, 127, 134*n*16, 137, 143, 144, 150–152, 157, 159–164, 166, 173, 175, 185*n*101, 185*n*102, 186, 198*n*151, 202*n*167, 204*n*179, 264, 265, 274, 279*n*94, 285–298, 300, 302–313, 306*n*96, 307–313, 325, 328, 329, 336, 345, 356, 367, 372, 373, 375*n*15, 376–381, 383–385, 388–390, 398, 411, 412, 426, 432–436, 438, 455, 456, 458, 474, 488, 495, 496, 499, 501–504, 510*n*51, 511–513, 514*n*60, 515*n*62, 522, 523, 528, 536, 537, 539, 541–545, 559, 582, 591, 610, 611, 614–616, 619, 648, 649, 651, 655, 660, 661, 663, 673–679, 680*n*44, 681–687, 690*n*127, 693–697, 699–708, 714, 716, 718*n*24, 721, 723, 724, 733*n*33, 755–762, 764–766, 772, 774, 782, 783, 788
tort 5, 6, 65, 77, 86, 87, 89, 91, 92, 141, 144, 145, 147, 191*n*118, 226, 227*n*57, 228–231, 274, 332, 338, 399–412, 413*n*86, 414–416, 578*n*104, 624, 625, 710, 745, 751, 752, 768, 771, 772, 780, 781

underlying assets 17, 38, 75, 111, 287, 289–291, 293, 298–300, 304, 307–310, 313, 374, 376, 377, 379, 380, 383–385, 396, 398, 678
universal jurisdiction 7, 570, 585–588, 602

Blockchain is the first global mechanism for the transfer and storage of value. Despite being conceived as an alternative to state and law, the technology and its use cases raise many legal questions, most notably, regarding jurisdiction and applicable law with respect to transactions and assets recorded on the blockchain. The issue is complex given the decentralised nature of the network. In this volume, academics and practitioners from various countries try to provide detailed answers to these questions as they relate to crypto-assets, cryptocurrencies, crypto derivatives, stablecoins, Central Bank Digital Currencies and Decentralised Autonomous Organisations (DAOs), as well as specific transactions and issues, such as property rights, secured transactions, smart contracts and bankruptcy. With specific chapters on national approaches (Germany, Japan, Liechtenstein, Switzerland, United States), the volume explores the need and possibility for legal harmonisation of these issues through global fora, such as the Hague Conference on Private International Law (HCCH) UNIDROIT.

Andrea Bonomi, PhD (1992 and 1994), is a Professor of Comparative Law and Private International Law at the University of Lausanne and the former Director of the Centre for Comparative, European and International Law. He is also a Director of the LL.M. in International Business Law.

Matthias Lehmann, PhD (2003 and 2011), Habilitation (Germany) (2008), is a Professor of Private, Private International and Comparative Law at the University of Vienna as well as Professor of European and Comparative Business Law at Radboud University Nijmegen. His main interest lies in cross-border and comparative aspects of banking and financial law.

Shaheeza Lalani, PhD (2011), University of Lausanne, is the Executive Director of the LL.M. Programme at the University of Lausanne. She has published many articles on Private International Law and Comparative Law and has edited several books on International Arbitration.

ISBN 978 90 04 51484 3
ISSN 2667-3495
brill.com/blpp