# Addressing Digital Vulnerability Through Private International Law

*Gérardine Goh Escolar*[*]

## *A. Introduction*

The token economy has powered the recent growth and mainstreaming of Web3 and its "potential to revolutionize agreements and value exchange",[1] leading to the birth of a novel user-led, user-owned economy. Web3 is defined by various parties as the "Read-Write-Own"[2] internet "owned by its builders and users, and orchestrated with tokens".[3] Forecasts increasingly predict that this Web3 economy is expected to outperform the traditional economy based on legacy institutions in various ways.[4]

The rapid advancement of digital technologies has outstripped any other innovation in history. Ubiquitous connectivity through mobile, internet-connected devices, and low-cost data storage, transfer and computing, have enabled new models for the delivery of services and the leveraging of large stores of data. As the largest user of digital technologies today, the financial sector represents a major driver in the digital transformation of the global economy, and will act as a catalyst in enabling equitable access to capital and finance,[5] a crucial step towards global financial inclusion.

---

* The author thanks Harry Cheng, Raquel Salinas Peixoto, Laura Molenaar, Philippine Chapot, Camilo Saldías Robles, Lwandle Mlalazi van der Niet and Ashlyn Cheong for their assistance. All opinions and any errors contained herein remain entirely those of the author and do not engage the organisations with which she is affiliated.

1 Shermin Voshmgir, *Token Economy: How the Web3 Reinvents the Internet* (2nd ed, Blockchain Hub Berlin 2020), 2.

2 Eshita, 'Web3: in a nutshell' (2021), https://eshita.mirror.xyz/H5bNIXATsWUv_QbbEz6lckYcgAa2rhXEPDRkecOlCOI, accessed 15 March 2024.

3 cdixon, 'Why Web 3 Matters', https://twitter.com/cdixon/status/1442201621266534402, (26 September 2021), accessed 15 March 2024, thread originated by @cdixon on Twitter (now X).

4 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*, (Elgar 2019), 93-111.

5 European Commission Fintech Action Plan, 8 March 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0109, accessed 15 March 2024.

Another recent trend is the widespread decoupling of use cases on distributed storage and transfer mechanisms such as distributed ledger technology (DLT). The decentralised storage and exchange of digital tokens, including through the use of DLT,[6] rely on a register or database split across an online network without a central control point.[7] Adding a further layer of complexity, many technologies are designed, developed and deployed on infrastructures or in spaces that remain beyond any single State's jurisdiction. The growing use of such distributed storage and transfer mechanisms has led to the validation and adoption of concrete, sector-specific use cases, as well as an acceleration of unique drivers of growth as a result of these use cases.[8] These can be seen in the expansion of DLT applications to various fields, including financial transactions, Internet of Things (IoT), and value and supply chains.[9] From cryptocurrency as the foundation of blockchain technologies relying on proof-of-work (PoW) protocol in Blockchain 1.0, Blockchain 2.0 moved on to smart contracts involving more financial functionality and decentralised applications with autonomously executing algorithms. This has further evolved into Blockchain 3.0, with larger-scale applications, improved performance, greater scalability and more interoperability, all rooted in proof-of-stake (PoS) protocol.[10]

---

6 See also the discussion about recent developments and trends in the digital economy, including DLT systems and applications, in HCCH, 'Developments with respect to PIL Implications of the Digital Economy', Prel. Doc. No 4 REV of January 2022, https://assets.hcch.net/docs/b06c28c5-d183-4d81-a663-f7bdb8f32dac.pdf, accessed 15 March 2024, paras 9-35.

7 UNCTAD, *Harnessing Blockchain for Sustainable Development: Prospects and Challenges*, (2021) UNCTAD/DLR/STICT/2021/3 and Corr. 1, p. 2.

8 See, *e.g.*, in the field of security in the Internet of Things, 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.

9 Marketwatch, 'Blockchain market size analytical overview, demand, trends and forecast to 2024', (2019) https://www.marketwatch.com/press-release/blockchain-market-size-analytical-overview-demand-trends-and-forecast-to-2024-2019-04-05, accessed 15 March 2024.

10 "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".
UNCTAD, *Harnessing Blockchain for Sustainable Development: Prospects and Challenges*, *supra* note 7, 4 and 52.

Activities and interactions across jurisdictions and borders often expose gaps in the legal framework, giving rise to vulnerabilities due to questions of private international law (PIL) that arise. These include questions as to which authority has jurisdiction, which law is applicable, how decisions are recognised and enforced, and what cooperation mechanisms are available to overcome challenges of cross-border judicial or administrative procedures. The growing digitisation of the global economy and community exacerbates these vulnerabilities, as digital creations, actions, transactions and reactions online are, by a large majority, cross-border interactions. The vulnerabilities that arise in a digital habitat are a result of the borderless, mostly instantaneous, digital exchanges that take place between actors and participants in online platforms. The recent explosion of DLT-based and DLT-enabled transactions and interactions only serve to create greater digital vulnerabilities due to the anonymity or pseudonymity of actors and participants, the lack of an obvious connecting factor to *situs* for many transactions, and the lacunae that exist as a result of a lack of a uniform, harmonised PIL framework.

### *B. Digital vulnerability in the context of private international law*

Vulnerability has emerged in various fields, from biomedical research and clinical medicine[11] to criminal justice,[12] as a core concept. The main idea is "an individual's (or a group's) propensity to suffer from physical or psychological harm".[13] From the perspective of legal scholarship, it can also be defined as the risk at which the rights of a person or group are violated.[14] Alarms have been sounded in the critical literature on vulnerability, with emphasis on the fact that the definition of vulnerability may either be too narrow (and hence run the risk of excluding individuals or groups

11 See generally Catriona Mackenzie, Wendy Rogers, Susan Dodds, *Vulnerability: New essays in ethics and feminist philosophy*, (2013: Oxford University Press); see also Samia A Hurst, 'Vulnerability in research and health care: describing the elephant in the room?', (2008) 22(4) Bioethics 191.

12 Robert Vargas, Kayla Preito-Hodge and Jeremy Christofferson, 'Digital Vulnerability: The Unequal Risk of E-Contact with the Criminal Justice System', (2019) 5(1) Russell Sage Foundation J Social Sciences 71.

13 Philipp Kellmeyer, 'Digital vulnerability: a new challenge in the age of super-convergent technologies', (2019) 12(1/2) Bioethica Forum 60 at p. 60.

14 Martha Albertson Fineman, 'The Vulnerable Subject: Anchoring Equality in the Human Condition', (2018) 2(1) Yale J of Law and Feminism, 1-24.

that may be vulnerable), or too broad (thus leading to a situation where a particular individual may be categorised as vulnerable despite not being especially so).[15] Vulnerability is therefore often complex and layered,[16] and transposing specific kinds of vulnerability that apply to the individual onto groups or populations remains a challenge in many fields.

This is particularly evident in the case of digital vulnerability, especially where mapped on to institutional vulnerabilities. "Digital vulnerability" relates to the manner and means of human interaction with digital technologies.[17] The aligned and accelerated "super-convergence" of complementary key digital technologies creates digital vulnerability as a result of the pervasiveness and ubiquity of their use.[18]

Digital vulnerabilities arise as specific PIL challenges in the different sectors of the digital economy. These include:

- applicable law and choice of law (*e.g.*, what is the most appropriate connecting factor defining the law applicable to a transaction on a cross-border online platform, or via blockchain);
- jurisdiction and choice of court (*e.g.*, how to determine the competent court to resolve a dispute in relation to a non-fungible token (NFT) transacted within an immersive technology platform);
- recognition and enforcement (*e.g.*, how to enforce a foreign judicial decision in relation to a service regulated by a smart contract); and
- cross-border and cross-platform cooperation mechanisms (*e.g.*, what co-operation frameworks are feasible and desirable to overcome challenges that the digital economy faces).

15 Catriona Mackenzie, Wendy Rogers, Susan Dodds, *supra* note 11.

16 Florencia Luna, 'Elucidating the concept of vulnerability: Layers not labels', (2009) 2(1) Int'l J of Feminist Approaches to Bioeithcs 121.

17 Such as the consequences, both legal and institutional, of deceptive illusions through immersive technologies, Philipp Kellmeyer, Nicola Biller-Andorno, Gerben Meynen, 'Ethical tensions of virtual reality treatment in vulnerable patients', (August 2019) 25(8) Nature Medicine 1185; see *infra* section C., VI.

18 Philipp Kellmeyer, *supra* note 13, 60.

### C. Practical use cases: answering private international law challenges to address digital vulnerability

Digital vulnerabilities that arise in the form of challenges to PIL are best illustrated in the practical use cases that abound in the digital economy today.[19] The protection of the rights of individuals, groups, businesses and communities begins with the question as to which framework of laws would be applicable, and run through to the question of which forum would be competent to hear a dispute, and how any resolution by the forum of such dispute would have practical effect. These form the classic trifecta of questions relating to applicable law, jurisdiction, and recognition and enforcement to which PIL addresses itself. In short, digital vulnerabilities arise because there is currently no harmonised framework that answers the what (law applies), when (such law should apply), who (should hear a dispute), and how (would parties have the opportunity to choose the law or forum) questions. From a PIL perspective, it is the *where* question (the *situs*) that may have traditionally aided in answering these other questions. It is the complexity – in some cases the impossibility – of answering the *where* question that gives rise to digital vulnerability.

The use cases that this section will examine are: (I) distributed storage mechanisms; (II) digital currencies and cross-border payments; (III) the tokenised economy; (IV) digital platforms; (V) artificial intelligence (AI) and automated contracting; (VI) immersive technologies and the cloud economy; and (VII) decentralised governance structures.

#### I. Distributed storage mechanisms

Increasingly, items and transactions take place online on distributed storage mechanisms, many of which are enabled by DLT. DLT has been defined as

19 See for more information in relation to studies undertaken on PIL aspects of these practical use cases, HCCH, 'Digital Economy and the HCCH Conference on Commercial, Digital and Financial Law Across Borders (CODIFI Conference): Report', Prel. Doc. No 3A of January 2023, https://assets.hcch.net/docs/a61a1225-2eb0-4fef-8a7e-24ca186b5919.pdf, accessed 15 March 2024; HCCH, 'Private International Law Aspects of the Digital Economy: Report', Prel. Doc. No 5A of February 2024, https://assets.hcch.net/docs/b74f3bfe-51dd-4d0e-8d4b-59e5e32367da.pdf, accessed 15 March 2024.

> "...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".[20]

DLT is the protocol on which blockchain applications are based. A register of payments ("ledger") distributed across an online network without a central control point is created by blockchain technology.[21] A network of computers cryptographically identifies users and validates interactions among them before recording the interactions across the network of identifying and validating computers.[22] 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. Each computer connected to the blockchain network is referred to as a node. Each of these nodes operates a full copy of validated transactions of the blockchain ledger.[23] Packages of data that carry the recorded data on the network are called "blocks". [24] 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.[25]

There are many ways of designing, implementing and employing DLT, which may be very different from the model used for blockchain. The unique design characteristics of DLT-enabled or DLT-native transactions

20 UNCTAD, *supra* note 7, 50.
21 *Ibid.*, 2.
22 See, *e.g.*, Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2008), https://bitcoin.org/bitcoin.pdf, accessed 15 March 2024, (the Bitcoin Whitepaper, explaining the basics of blockchains); Vitalik Buterin, 'A next-generation smart contract and decentralized application platform', (2013), https://finpedia.vn/wp-content/uploads/2022/02/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf, accessed 15 March 2024, (the Ethereum Whitepaper, elaborating on the functioning of blockchains as well as smart contracts).
23 UNCTAD, *supra* note 7, 51.
24 *Ibid.*, 50.
25 *Ibid.*

and systems strain the application of traditional connecting factors.[26] Traditional connecting factors are difficult to apply to these technologies, with technological and legal challenges based on the pseudonymity of users, the immaterial nature of digital assets, the uncertainty of the location of network nodes and the online or decentralised nature of the platforms, making it difficult, or perhaps impossible, to determine the *situs* of a participant, item or transaction.[27]

Some DLT-enabled platforms further complicate the matter by resisting formal regulation in favour of self-regulation or adherence to the ethos of *lex cryptographica*.[28] Other PIL issues that arise in DLT use cases include:[29]

- the characterisation of, and law applicable to, the relationship between participants in a DLT system, including between asset holders and intermediaries such as crypto-exchanges and wallet providers;
- the law applicable to, the holding and transacting of assets in a DLT system;
- the jurisdiction of courts to hear disputes related to the outcomes of self-executing smart contracts deployed in DLT systems;
- the recognition and enforcement of DLT-based dispute resolution outcomes; and
- the question of how to determine the law applicable to tokens linked to real-world assets.

---

26 HCCH, Prel. Doc. No 3A of January 2023, *supra* note 19. See also the discussion about connecting factors in relation to digital assets created and transferred via decentralised systems, in HCCH, 'Developments with respect to PIL implications of the digital economy, including DLT', Prel. Doc. No 4 of November 2020, https://assets.hcch.net/docs/8bdc7071-c324-4660-96bc-86efba6214f2.pdf, accessed 15 March 2024, paras 15-21.

27 Matthias Lehmann, 'Who Owns Bitcoin? Private (International) Law Facing the Blockchain', (2019) 42 *European Banking Institute Working Paper Series 2019*, 2.

28 See, *e.g.*, Primavera de Fillippi and Aaron Wright, *Blockchain and the Law – The Rule of Code* (Harvard University Press 2018). For an opposite view, see David Sindres, 'Is Bitcoin out of Reach for Private International Law?', in Andrea Bonomi, Matthias Lehmann, Shaheeza Lalani (eds), *Blockchain and Private International Law* (Brill Nijhoff 2023) 81.

29 Gérardine Goh Escolar, 'The Role and Prospects of Private International Law Harmonisation in the Area of DLT', in Andrea Bonomi, Matthias Lehmann, Shaheeza Lalani (eds), *Blockchain and Private International Law* (Brill Nijhoff 2023) 10. See also the discussion about the different PIL implications of permissioned and permissionless systems, in HCCH, Prel. Doc. No 4 of November 2020, *supra* note 26, para. 16 and Annex I.

The characteristics of each DLT system impact the use cases best suited to it and raise different PIL issues.[30] Without an explicit choice of the applicable law, obstacles to the application of traditional objective connecting factors include the pseudonymity of the users and the inability to locate the DLT platform's connections to a certain jurisdiction, though some authorities have made attempts to do so based on the concentration of nodes.[31] While the explicit determination of the applicable law in an online platform agreement would be ideal, it does not consistently account for circumstances where users choose to avoid the services of a centralised platform, for reasons including security concerns, lack of platform trust, and personal philosophy. This has led to differing views as to whether analogies can be drawn from legal frameworks in existing regimes such as intellectual property[32] or goodwill in a business,[33] or whether an entirely new approach should be taken.[34] Moreover, the regulatory perimeters of many domestic legal institutions have been deemed to be insufficient to address the difficulties raised by the cross-border nature of DLT-enabled systems and applications. The larger-scale applications serviced by Blockchain 3.0 may also mean that "[n]o one solution can fit all DLT systems".[35]

30 On the use case analysis of DLT by asset class and product line, see World Economic Forum, *Digital Assets, Distributed Ledger Technology and the Future of Capital Markets: Insight Report*, (May 2021) https://www3.weforum.org/docs/WEF_Digital_Assets_Distributed_Ledger_Technology_2021.pdf, accessed 15 March 2024, 32-86.

31 Matthias Lehmann, 'Who Owns Bitcoin? Private (International) Law Facing the Blockchain', (2019), *supra* note 27.

32 Gerald Spindler, 'Fintech, digitalization, and the law applicable to proprietary effects of transactions in securities (tokens): a European perspective', (2019) 24 ULR 336, 337.

33 Andrew Dickinson (2019), 'Cryptocurrencies and the Conflict of Laws', in David Fox and Sarah Green (eds), *Cryptocurrencies in Public and Private Law* (Oxford University Press 2019), paras 5.107–5.121.

34 See generally Michael Ng, 'Choice of law for property issues regarding Bitcoin under English law', (2019) 15(2) J Private Intl Law 316.

35 Financial Markets Law Committee (2018), *Distributed Ledger Technology and Governing Law: Issues of Legal Uncertainty*, (2018), 21.

## II. Digital currencies and cross-border payments

Digital currencies are a "digital version of cash, controlled by a private cryptographic key – a unique random string of numbers".[36] 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: Cryptocurrencies (*e.g.* Bitcoin, Ethereum, Solana); StableCoins (*e.g.* Diem, formerly Libra), which are backed by a reserve asset such as fiat currency[37] held by banks; and Central Bank Digital Currencies (CBDCs), which are digital versions of fiat issued by a country's central bank.

In relation to cryptocurrencies, specific objections have been raised to the application of traditional PIL frameworks to legal relationships involving the use of cryptocurrencies. Arguments include views that these relationships are self-regulated and are subject to the *lex cryptographica* as opposed to legal regulation such as *lex mecatoria*,[38] or that there are major obstacles to the application of PIL in this field, including the delocalisation of transactions and the pseudonymity of actors.[39] Objections have been framed along two lines – either by viewing cryptocurrencies as assets in the sense of intangible movable property or by viewing cryptocurrencies as currency, and applying PIL by analogy.[40] Some commentators have moreover argued that the rapid evolution and diversification of the crypto asset and cryptocurrency landscape means that choice of law rules should offer "a sufficient degree of flexibility along with legal foreseeability and

36 Visa, 'The Crypto Phenomenon: Consumer Attitudes & Usage', (2021) https://usa.visa.com/content/dam/VCOM/regional/na/us/Solutions/documents/visa-crypto-consumer-perceptions-white-paper.pdf, accessed 15 March 2024, 7.

37 "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, World Bank, 'Bitcoin versus Electronic Money', (2014) https://documents1.worldbank.org/curated/en/455961468152724527/pdf/881640BRI0Box30WLEDGENOTES0Jan02014.pdf, accessed 15 March 2024, 1.

38 See *supra* note 28.

39 See, *e.g.*, M. Audit, 'Le droit international privé confronté à la blockchain', (2020) Rev crit DIP 669, 689.

40 See, *e.g.*, David Sindres, 'Is Bitcoin out of Reach for Private International Law?', *supra* note 28.

certainty".[41] Here, one solution may be to allow for the principle of party autonomy in choice of law,[42] which would enable parties to agree on the law governing the relationship between them, while accepting that there may be certain limitations on the freedom of choice in this context.[43]

On the other hand, CBDCs are digital currencies[44] issued by central banks, which include as key features: (1) the designation as a central bank liability; (2) denomination in an existing unit of account; and (3) use as a medium of exchange and a store of value.[45] Countries may have different objectives in issuing CBDCs, which include improving access to payments and promoting financial inclusion, increasing payment system competition, efficiency, and resilience, as well as safeguarding monetary sovereignty, and monetary and financial stability.[46] In 2022, it was estimated that 93% of central banks were exploring CBDCs, and that 58% were considering issuing a retail CBDC in either the short or medium term.[47] Use cases of CBDCs in finance, trade and digitised commerce include cross-border payments, e-commerce, machine-to-machine transactions and smart contracts.

41 Burcu Yüksel Ripley and Florian Heindler, 'The Law Applicable to Crypto Assets: What Policy Choices are Ahead of Us?', in Andrea Bonomi, Matthias Lehmann, Shaheeza Lalani (eds), *Blockchain and Private International Law* (Brill Nijhoff 2023) 259.

42 Simoen C Symeonides, *Codifying Choice of Law Around the World: An International Comparative Analysis*, (Oxford University Press 2014), Chapter 3.

43 See, *e.g.*, HCCH, Prel. Doc. No 4 of November 2020, *supra* note 26, Annex I.

44 The Bank for International Settlements (BIS) provides a succinct explanation of CBDCs, noting that there are two types of CBDCs, "[r]etail CBDCs (rCBDCs) are intended for the general public, aiming to provide a risk-free and digital means of payment for everyday transactions. Wholesale CBDCs (wCBDCs), on the other hand, are designed for use among financial intermediaries and operate like central bank reserves but with added functionalities enabled by tokenisation". See BIS / FSI Connect, "Central bank digital currencies – Executive Summary", undated, https://www.bis.org/fsi/fsisummaries/cbdcs.pdf, accessed 15 March 2024.

45 IMF WP/20/254, 'Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations', (November 2020), 6. A possible indirect structure is the issuance of the liability by a commercial bank which in turn is fully backed with central bank liabilities. This structure is not deemed as a genuine CBDC by some experts, because in the case of bankruptcy of the commercial bank the user would have a claim against such commercial bank, not against the central bank.

46 Gabriel Soderberg, *et al*., IMF NOTE/2023/008, 'How should central banks explore central bank digital currency?' (September 2023), https://www.imf.org/en/Publications/fintech-notes/Issues/2023/09/08/How-Should-Central-Banks-Explore-Central-Bank-Digital-Currency-538504, accessed 15 March 2024, 9-11.

47 BIS, BIS PAPER/23/136, 'Making headway – Results of the 2022 BIS survey on central bank digital currencies and crypto', (2023), 4 and 9.

A PIL analysis of the use of CBDCs could generally start with the use of traditional connecting factors. Potential connecting factors may depend on the infrastructure where a CBDC is issued. For example, a possible infrastructure could be on a distributed ledger located in multiple jurisdictions and without either a central authority or validation point, where applying the *lex situs* or the Place of Relevant Intermediary Approach (PRIMA) principle as a connecting factor may be difficult, especially in relation to intangible assets held therein.[48] While the implications of a certain infrastructure can presumably be clarified by the supervision of the central bank or another authority that is able to designate an applicable law to the system, the *situs* becomes less clear where, for example, the central bank's role is limited to identity verification or where technical ledger access and intermediaries play a greater role.[49] Other connecting factors include the law chosen by the DLT network participants (*elective situs*), the law approved by regulators (*modified elective situs*), the residence of the participant who is transferring the CBDC or the residence of the encryption private master key-holder for the DLT system (PREMA).[50]

The legal nature of CBDCs might also pose challenges to applying conventional PIL rules.[51] Even if rules are found to apply, it is not clear whether every existing rule is fit for purpose. For example, if a CBDC is classified as a tangible-intangible hybrid under a domestic legal framework, the *lex rei sitae* could in theory apply, but it is unclear what the *situs* of a token held on distributed registers and through wallets would be.[52]

CBDCs have the potential to alleviate existing frictions caused by a lack of interoperability, standardisation, as well as other challenges (*e.g.*, high number of intermediaries) in cross-border payments,[53] which are financial transactions where the payer and the recipient are based in different

48 See HCCH, Prel. Doc. No 4 of November 2020, *supra* note 26.

49 See HCCH, 'Exploratory Work: Private International Law Aspects of Central Bank Digital Currencies (CBDCs)', Prel. Doc. No 4 of January 2024, https://assets.hcch.net/docs/410f9f34-3360-4d22-87ff-0876377a3d87.pdf, accessed 15 March 2024, Annex III. An example is Project Tourbillon, see Annex IV.

50 *Ibid.* Previous exploratory work carried out by the Permanent Bureau of the HCCH already has identified connecting factors in the context of digital economy, including DLT, and could be a relevant input for future work, see Annex I, HCCH, Prel. Doc. No 4 of November 2020, *supra* note 26.

51 HCCH, Prel. Doc. No 4 of January 2024, *supra* note 49, para. 55.

52 *Ibid.*

53 BIS, BIS Report to the G20 *Central bank digital currencies for cross-border payments*, (July 2021), 13-14.

jurisdictions.[54] Here again, PIL challenges will need to be answered. An example is the issuance and use of a CBDC as a digital token without a current-account relationship between the central bank and the holder,[55] and where intermediaries may provide services such as holding wallets and handling payments for users.[56] Many national legislations do not recognise CBDCs as a form of digital asset, as CBDCs and digital assets serve different purposes and have different legal implications.[57] As such, crucial legal implications arise in the design choices underlying a CBDC.[58]

Depending on the chosen design and model of operation, particularly in relation to cross-border CBDC access by non-residents, central banks may delegate functions to private sector intermediaries.[59] Deployment of national CBDCs may also potentially require the use of foreign intermediaries, or intermediaries with worldwide offices; moreover, a user may hold CBDCs of different jurisdictions in the same account. Intermediaries provide necessary services for the operation and implementation of CBDCs but the functions delegated to them, their location, and their method of integration into the CBDC system may raise PIL issues. Intermediaries may be afforded varying degrees of functionality and independence depending on how they are included in the technical framework of a CBDC cross-border payment system, leading to complexities in the analysis of *situs*. Thus, the PIL implications resemble the intermediation and dematerialisation challenges that informed the development of the *Convention of 5 July 2006 on the Law Ap-*

54 IMF NOTE/2023/008, *supra* note 46, 10, 20-21, about CBDCs used for cross-border payments.

55 IMF, IMF WP/20/254 *Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations*, (November 2020), 9.

56 HCCH, Prel. Doc. No 4 of January 2024, *supra* note 49. It may be too challenging for central banks to assume such tasks. Accordingly, intermediaries, such as commercial banks and financial institutions, are considered as more suitable for it.

57 HCCH, Prel. Doc. No 4 of January 2024, *supra* note 49.

58 In WP/20/254, *supra* note 55, 10-11. the IMF has identified these choices on CBDC design in terms of dichotomies between account-based vs. token-based; wholesale vs. retail; direct vs. indirect; and centralised vs. decentralised. In addition, in IMF NOTE/2023/008, *supra* note 46, 18-19, the IMF noted that different principles may be considered to assess the design options, such as interoperability, compliance with the laws and regulations, resiliency, upgradability, and others.

59 BIS, *Options for access and interoperability of CBDC for cross-border payments*, (2022), https://www.bis.org/publ/othp52.pdf, accessed 15 March 2024.

*plicable to Certain Rights in Respect of Securities held with an Intermediary* (HCCH Securities Convention).[60]

Clarity as to applicable law considerations in payment systems interoperability would enable payments service providers to make payments across systems without concerns as to payments law and settlement finality. As CBDCs systems used for payments would have similarities with existing payments infrastructure, existing payments law may be a useful starting point for establishing PIL considerations.[61]

However, the specific features of CBDCs do not allow the PIL frameworks that already exist for cash payments to apply one-to-one. For example, the *lex monetae* could prevail over party autonomy when determining the applicable law for some issues. Additionally, the participation of intermediaries would have an impact on the PIL analysis. Recipient countries of a foreign CBDC could decide the extent to which they will authorise the denomination of contracts in foreign currency, and recipient countries' treatment of a foreign CBDC is likely to be affected by the issuing country's rules regarding that CBDC.[62] These PIL challenges would arise in both wholesale retail payments within the specific context of each country or jurisdiction.[63] Notably, the roles and responsibilities of intermediaries in cross-border payments and the status of intermediaries in cross-border insolvency regimes are issues that should be considered in any PIL analysis.[64]

---

60 HCCH *Convention of 5 July 2006 on the Law Applicable to Certain Rights in Respect of Securities held with an Intermediary*, https://assets.hcch.net/docs/3afb8418-7eb7-4a0c-af85-c4f35995bb8a.pdf, accessed 15 March 2024.

61 HCCH, Prel. Doc. No 4 of January 2024, *supra* note 49.

62 Heng Wang, 'How to Understand China's Approach to Central Bank Digital Currency', (2023) 50 Computer Law and Security Rev 1, 24. Such PIL considerations, of course, would be subject to overriding mandatory regulations and other overriding considerations including monetary sovereignty, foreign exchange policies, and other regulatory and compliance requirements.

63 There are pilots on both use cases: wholesale payments and retail payments. Cross border pilots have been mostly focused on wholesale payments, in collaborative projects carried out by groups of central banks. Moreover, some central banks are more active in implementation or experimentation of CBDC pilots, while others are more cautious. These differences are mainly explained because the design of a CBDC needs to address the specific context of each country, and some central banks have not identified the need to introduce a CBDC, thus conducting monitoring activities while others prefer the involvement of private parties (*e.g.*, commercial banks) in more advanced stages. Regarding the country-specific circumstances to be considered for a CBDC design, see BIS Innovation Hub, 'Project Polaris Part 4: A high-level design guide for offline payments with CBDC', (October 2023), 33-37.

64 HCCH, Prel. Doc. No 4 of January 2024, *supra* note 49.

## III. The tokenised economy

Digital tokenisation allows tangible and intangible objects, rights and claims to be virtually represented and stored electronically, usually in distributed storage mechanisms. While recognising the lack of such a definition, the BIS notes that tokenisation refers to the digital representation of value or rights.[65] Tokenisation can be an enabler of fast and secure transactions, including transfers, tracking and management of tokenised value or rights across borders. According to the BIS, tokenisation streamlines transactions, reducing the need for intermediaries and increasing the transparency and security of these transactions. Consequently, digital tokenisation has become one of the most prominent use cases of distributed storage mechanisms in financial and capital markets in many jurisdictions.

Three trends are of particular interest.

The first trend is the digital tokenisation of real-world assets by the creation of a virtual representation of existing tangible assets,[66] storing these virtual representations on decentralised or distributed storage mechanisms (for example, using DLT), and conventionally embedding their value and any rights or obligations associated with the real-world asset in the virtual representation.[67] This may include the representation on DLT of traditional asset classes such as financial instruments, collateral or real assets.[68] The relevant real-world assets, in particular where they are tangible assets, would typically be placed in custody to ensure continuous backing for the

65 BIS, Annual Economic Report Part III, (June 2023) https://www.bis.org/publ/arpdf/ar2023e3.pdf, accessed 15 March 2024, 89.

66 Garrick Hilleman and Michel Rauchs, Global Blockchain Benchmarking Study, (2017) https://dx.doi.org/10.2139/ssrn.3040224, accessed 15 March 2024, 51 and 64.

67 *Ibid*., see also Iñaki Aldasoro *et al*., The tokenisation continuum, 11 April 2023, https://www.bis.org/publ/bisbull72.pdf, accessed 15 March 2024, 1, 3. Tokenisation may include, for example, "the representation of pre-existing real assets on the ledger by linking or embedding by convention the economic value and rights derived from these assets into digital tokens", see Organisation for Economic Co-operation and Development (OECD), *The Tokenization of Assets and Potential Implications for Financial Markets*, (2020) OECD Blockchain Policy Series, https://www.oecd.org/finance/The-Tokenisation-of-Assets-and-Potential-Implications-for-Financial-Markets.htm, accessed 15 March 2024, 11.

68 See, for example, Financial Stability Board (FSB), *Decentralised financial technologies: Report on financial stability, regulatory and governance implications*, (2019), https://www.fsb.org/wp-content/uploads/P060619.pdf, accessed 15 March 2024.

digital tokens. Tokenisation is currently being piloted for various real-world assets, such as real estate.[69]

According to the OECD,

> "[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".[70]

Nevertheless, the OECD goes on to note that the large-scale adoption of asset tokenisation would face "governance risks related to AML/CFT;[71] digital identity issues; and data protection and privacy issues; as well as rais[e] questions about the legal status of smart contracts".[72] Questions relating to the characterisation of such tokens for PIL purposes, and the significant role of custodianship of assets that have been tokenised, will necessarily arise.

An example of such asset tokenisation relates to NFTs. NFTs form 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.[73] The European Union Blockchain Observatory and Forum has noted that indicative NFT use

69 OECD, *The Tokenization of Assets and Potential Implications for Financial Markets*, (2020), *supra* note 67.

70 *Ibid*., 7.

71 AML/CFT is the acronym for "anti-money laundering/combating the financing of terrorism".

72 OECD, *The Tokenization of Assets and Potential Implications for Financial Markets*, (2020), *supra* note 67, 7.

73 EU Blockchain Observatory and Forum, 'Demystifying Non-Fungible Tokens (NFTs)' (November 2021), 4-5.

cases include digital art[74] (including gaming collectibles),[75] supply chain logistics,[76] content ownership,[77] and assets in immersive technologies.[78]

A specific issue that NFTs face is the recognition and enforcement of the underlying mechanism used for transferring and establishing ownership. While some have opined that NFTs are property deeds that give an ownership title to a physical asset,[79] the deed or title entitles the holder to ownership of the asset and is not the asset itself. The purchase of an NFT gives ownership of the NFT itself, with any further rights or entitlements decided by the terms of the token smart contract. This raises the question of the characterisation of NFT transactions – whether they are solely contractual, or whether they carry proprietary characteristics. Other issues

74 See, *e.g.*, Beeple (2021), 'Everydays: The First 5000 Days', minted on 16 February 2021 and sold at online auction on 11 March 2021 for in excess of USD 69 million, https://onlineonly.christies.com/s/beeple-first-5000-days/beeple-b-1981-1/112924, accessed 15 March 2024.

75 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, https://www.cryptokitties.co/, accessed 15 March 2024.

76 See, *e.g.*, Nike's Cryptokicks project, for which it secured a patent, that stores unique identifiers given to each pair of shoes, https://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=1&f=G&l=50&co1=AND&d=PTXT&s1=Nike&s2=Crypto&OS=Nike+AND+Crypto&RS=Nike+AND+Crypto, accessed 15 March 2024.

77 See, *e.g.*, Audius, a decentralised audio streaming and sharing platform on the blockchain, https://audius.co/, accessed 15 March 2024.

78 See, *e.g.*, sales of digital land in the Sandbox and Decentraland, Cointelegraph, 'Virtual land in the metaverse dominated NFT sales over past week' (6 December 2021), https://cointelegraph.com/news/virtual-land-in-the-metaverse-dominated-nft-sales-over-past-week, accessed 15 March 2024.

79 Jeremy Goldman, 'A Primer on NFTs and Intellectual Property' (March 2021), https://www.lexology.com/library/detail.aspx?g=d96ed012-8789-4e87-bc1d-70ba76569c0f, accessed 15 March 2024.

that arise in regard of characterisation is whether NFTs can be considered commodities,[80] securities,[81] or intellectual property.[82]

The second trend relates to the focus on fund tokenisation. These "digital funds" issue tokenised shares or units that represent investor interests, which are recorded and traded on distributed platforms rather than in the traditional registries or record-keeping systems.[83] Such digital funds have gained traction in leading fund jurisdictions worldwide, including France, Germany, Luxembourg, Singapore and the United States of America.[84] An example of a cross-jurisdictional tokenised fund is the collaboration between the BIS Innovation Hub, the Swiss National Bank, the World Bank and the International Monetary Fund (IMF) to tokenise development funds, with the goal of promoting global economic development.[85]

The digital nature of these tokenised funds, compounded by their storage on distributed storage mechanisms, raises issues of localisation that have an impact on the PIL analysis. The variety of actors and participants in transactions involving digital tokens may challenge the application of traditional connecting factors, as there may be several objective connecting factors to a number of jurisdictions. The digital nature of this field also means that transactions may occur, and participants may be sited, in different jurisdic-

80 See, *e.g.*, the U.S. Commodity Futures Trading Commission (CFTC), CFTC (2020), *Digital Assets Primer,* https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwi0uoe5_Ob0AhWp7rsIHc9ODKAQFnoECCAQAQ&url=https%3A%2F%2Fwww.cftc.gov%2Fmedia%2F5476%2FDigitalAssetsPrimer%2Fdownload&usg=AOvVaw0ldGq63IE48QOEzXajIyBa, accessed 15 March 2024.

81 See, *e.g.*, the position of the U.S. Securities and Exchange Commission (SEC), SEC (2021), 'Framework for 'Investment Contract' Analysis of Digital Assets', https://www.sec.gov/files/dlt-framework.pdf, accessed 15 March 2024.

82 Amy Madison Luo, 'NFTs: A Legal Guide for Creators and Collectors', (11 March 2021), https://www.coindesk.com/policy/2021/03/11/nfts-a-legal-guide-for-creators-and-collectors/, accessed 15 March 2024.

83 Investment Association, *UK Fund Tokenisation: A Blueprint for Implementation. Interim Report from the Technology Working Group to the Asset Management Taskforce*, (November 2023), https://www.theia.org/sites/default/files/2023-11/UK%20Fund%20Tokenisation%20-%20A%20Blueprint%20for%20Implementation.pdf, accessed 15 March 2024, 9.

84 *Ibid*., p. 16.

85 Cecilia Skingsley, Head of the BIS Innovation Hub, 'Shaping the future financial system in the public interest', Keynote Speech at the Conference "Exploring central bank digital currency: Evaluating challenges & developing international standards", (28 November 2023), Washington DC, https://www.bis.org/speeches/sp231128.htm, accessed 15 March 2024, para. 50.

tions and locations. PIL questions regarding which law would be applicable and which forum would have jurisdiction would necessarily arise.

The third trend relates to the tokenisation of identity-bound data. This finds its use case in the issuance of soulbound tokens.[86] Soulbound tokens are defined as publicly-visible, non-transferable tokens representing affiliations, memberships, and credentials, enabling a digital DLT wallet to act as an "extended resumé" of the holder's activities and relationships.[87] Illustrations include tokens issued by a university to certify that the wallet holder is a graduate, tokens providing proof of substantial relationships such as participation in the governance of decentralised autonomous organisations (DAOs), and tokens used to model traditional financial systems and arrangements.

These soulbound tokens provide a digital method of representing a wallet holder's location, personal identification, or affiliations. An elaborated arrangement of soulbound tokens could provide an indication of real-world identities, locations, places of business, and patterns of social or economic behaviour, all of which are facts that facilitate the application of traditional connecting factors. Furthermore, users would be incentivised to voluntarily acquire more soulbound tokens because their possession can signal the authenticity of their own digital wallets and the consistency and reliability of their performance of obligations. Such markers of reliability in a wallet would facilitate access to more privileges for the holder. For this reason, soulbound tokens may overcome the location- and identity-based barriers of PIL and DLT, while respecting the ethos of peer-to-peer exchange that guides many DLT communities.

86 E. Glen Weyl, Puja Ohlhaver, Vitalik Buterin, 'Decentralized Society: Finding Web3's Soul', (2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4105763, accessed 15 March 2024.

87 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.

## IV. Digital platforms

Digital platforms refer to "digital infrastructure enabling interaction among multiple groups".[88] Digital platforms operate across varied sectors, enabling different types of interactions between different categories of parties. PIL issues manifest in various ways in the platform economy, depending on the relationships that arise:[89]

- Between the platform and the user: The relationship between the platform and the user typically is contractual and, of relevance to PIL, typically relies on choice of law clauses;
- Between users: Questions arise where there is no valid choice of law, as is often the case in peer-to-peer digital environments;
- Between the platform and / or its user, and the non-user: Where there are no pre-existing relationships between these parties, questions may arise where a harm is done to the non-user, in particular in relation to tortious claims. There may also be questions in relation to the law applicable to the determination of the liability of intermediaries.[90]

In relationships between platforms and their users, three specific PIL issues arise. First, the determination of the law applicable to contracts between the platform and the user is generally straightforward. However, tortious matters give rise to questions of the law applicable, as a rule for the law applicable based on the place of the user's location or the user's habitual residence may conflict with the contractual terms of the platform. Second, there is an increasing number of cases that are being litigated between aggrieved users and online platforms in which user-plaintiffs have argued that, where they have suffered a wrong done by another user, platform hosts are obliged to either sanction the (allegedly) offending user or otherwise remedy the wrong. The question that arises is whether choice of court and choice of law clauses in contracts entered into between users and the relevant digital platforms may go some way towards resolving such questions.[91] Third, and perhaps most significant in the discussion of digital

88 See Dai Yokomizo, 'Digital Platforms and Conflict of Laws', (2021) 64 Japanese Yb of Int'l Law 202, 202.

89 See Tobias Lutzi, 'Private ordering, the platform economy and the regulatory potential of private international law', in Ilaria Pretelli (ed.) *Conflict of Laws in the maze of digital platforms*, (Schultess: 2018), 129-143.

90 See Dai Yokomizo, *supra* note 88, 216.

91 *See* Tobias Lutzi, *supra* note 89, 134.

vulnerability, while some jurisdictions have specific PIL rules that protect weaker parties such as consumers and employees, these sector-specific rules do not apply to protect the small and medium-sized enterprises that also take part in transactions on digital platforms, leaving a lacuna in the PIL framework.[92]

The fastest-growing use case of digital platforms, in particular on distributed storage mechanisms, is decentralised finance (DeFi). DeFi platforms bring together a wide spectrum of financial market participants and has been attracting significant capital and liquidity pools in the international and cross-border financial ecosystem. DLT-enabled DeFi platforms operate without a centralised authority or physical presence, and their transactions can be executed automatically, thereby imposing challenges in connecting a transaction on a DeFi platform to a location for the determination of jurisdiction and applicable law through the use of traditional connecting factors.

## V. Artificial intelligence and automated contracting

The adoption of AI in applications, in particular generative AI, has led to innovations in various fields, such as automated contracting. While automated contracting is not new, having been the basis of applications such as point-of-sale systems and electronic data interchange (EDI) for many decades, the use of automated contracting in smart contracts, computable contracts, and algorithmic contracts has meant an increased reliance on AI in both commercial and end-user contracts. In particular, transactions conducted on online platforms and smart devices (including high-frequency trading transactions) can involve interactions between a human and an automated system, or interactions between automated systems. Automation at the different stages of the contract life cycle, together with the automation of stages in the contract life cycle from drafting to negotiation and

92 Most of these laws enable the use of a specific mandatory rule of law from the jurisdiction in which these weaker parties are habitually resident, see Dai Yokonizo, *supra* note 88, 225.

management to analysis,[93] allow for the streamlining and systematising of cross-border contracting on digital platforms.

Developments in AI and automated contracting have raised several PIL questions. First, when AI-enabled technologies perform acts or take part in transactions, the online nature of most AI-enabled systems may make traditional connecting factors inapplicable. Second, the use of AI-enabled systems may make determining jurisdiction difficult due to the challenges in determining location in online platforms (including the application of the *forum non conveniens* doctrine, where relevant). Another challenge relates to the identification of the type of harm that an AI-enabled system may cause, and to the localisation of such harm, since traditionally *situs*-based PIL connecting factors may not be useful in linking the occurrence of the damage to a certain jurisdiction. For example, a generative AI-enabled networked system not localised to a particular *situs* may scrape data from one website in a particular jurisdiction in order to generate content on another website sited elsewhere.[94] Third, the enforcement of foreign judgments may be challenging as a result of different approaches to AI-enabled systems. Some jurisdictions may see public policy and other concerns presenting obstacles to the recognition and enforcement of decisions in situations where AI-enabled algorithms are involved, and where they are empowered to render final decisions.

## VI. Immersive technologies and the cloud economy

Immersive technologies have created virtual multi-purpose platforms that are empowered by virtual and augmented reality and methods of transacting based on distributed storage mechanisms. Such platforms based on immersive technologies, in particular those native to the cloud, allow individuals, businesses and other entities to create, act, react and transact in relation to both real-world as well as virtual items. Immersive technologies have found applications in a range of use cases that include enter-

93 See Martin Ebers, 'Artificial Intelligence, contracting and contract law' in Martin Ebers, Cristina Poncibò, Mimi Zou (eds.), *Contracting and contract law in the age of artificial intelligence*, (2022: Bloomsbury) 102.

94 Marion Ho-Dac, and Cécile Pellegrini, *Governance of Artificial Intelligence in the European Union: What Place for Consumer Protection?*, (Bruylant: 2023), 303.

tainment,[95] gaming,[96] litigation and arbitration proceedings,[97] and digital communications.[98] Web3 immersive technology platforms 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".[99] These platforms create a new paradigm by eliminating capital controls and creating a "new free-market internet-native economy that can be monetised in the physical world",[100] a revenue opportunity that spans social commerce, digital events, hardware, and content monetisation.[101]

Immersive technologies raise PIL questions not only because of the nature of the networked platforms on which these technologies operate, but also as a result of the seamless connection between digital and real-world objects. Here, traditional connecting factors may not apply, leading to challenges in identifying the applicable law (which may address the platform as a whole, or may address a single transaction or user), and the possible anonymity or pseudonymity with which users interact in immersive technology platforms. It therefore becomes a challenge to connect events, assets,

95 For example, over 12 million users joined the Fortnite platform to watch a virtual concert by entertainer Travis Scott in April 2020, see Ji Hye Park, 'The Direction and Implications of the Content Industry in the Metaverse Era', (2022) 26(6) *KIET Industrial Economic Review* 55, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4194255, accessed 15 March 2024.

96 The number of monthly users of Roblox, an immersive technology game, exceeds 150 million, see Busra Alma Çalli and Cagla Ediz, 'Top concerns of user experiences in Metaverse games: a text-mining based approach', (May 2023), 46 Entertainment Computing, https://www.sciencedirect.com/science/article/abs/pii/S1875952123000319, accessed 15 March 2024.

97 Timothy T Hsieh *et al.*, 'Intellectual Property in the Era of AI, Blockchain and Web 3.0', (March 2023), *Blockchain and Web* 3, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4392895, accessed 15 March 2024.

98 See generally Dale Mitchell, Ashley Pearson and Timothy D Peters (eds.), *Law, Video Games, Virtual Realities: Playing Law*, (Routledge 2024).

99 Grayscale Research, 'The Metaverse: Web 3.0 Virtual Cloud Economies' (2021), https://grayscale.com/wp-content/uploads/2021/11/Grayscale_Metaverse_Report_Nov2021.pdf, accessed 15 March 2024, 10.

100 *Ibid.*, 7.

101 Grayscale Research, 'The Metaverse', *supra* note 99, 9 and 16. See also Pedro Palandrani, The Metaverse Takes Shape as Several Themes Converge, *Global X ETFs Research,* (13 September 2021), https://www.globalxetfs.com/content/files/The-Metaverse-Takes-Shape-as-Several-Themes-Converge.pdf, accessed 15 March 2024.

and actors where they may not have (validly) agreed on applicable laws and jurisdiction.[102]

Immersive technology at play in cloud economies raise questions in relation to the characterisation of the agents relating to sovereign virtual goods being transacted in the cloud. Questions arise as to the legal frameworks that are relevant, and the PIL implications of those legal frameworks. Perhaps most significant in relation to the use of immersive technologies in cloud economies is the increasing use of decentralised governance, including decentralised autonomous organisation (DAO) frameworks and their attendant voting mechanisms, community audits, and multisignature wallets.[103] Decentralised cloud services also mean that storage, computing, and databases are decentralised in the borderless cloud. The borderless nature of cloud economies finds itself in tension with the traditional significance of geographic *situs* in PIL.[104]

Another issue that arises in cloud economies and metaverses is the PIL implications of cross-border data transactions. While the general focus of regulators has thus far been on consumer privacy and the protection of personally identifiable data,[105] PIL questions relating to jurisdiction, applicable law and recognition will increasingly arise as more data transactions take place in the cloud and as certifications of data transactions are increasingly tokenised.

---

102 See generally European Parliament, Briefing: Metaverse Opportunities, risks and policy implications, (June 2022), https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733557/EPRS_BRI(2022)733557_EN.pdf, accessed 15 March 2024; see also Grayscale Research, 'The Metaverse', *supra* note 99.

103 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 wallet commonly used in DAOs, see, *e.g.*, Monika di Angelo and Gernot Salzer, 'Characteristics of Wallet Contracts on Ethereum', (2020) *IEEE* 1, 1-2. See *infra* section C., VII.

104 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; see also Gérardine Goh Escolar, *supra* note 29.

105 Jin Huang, 'Applicable Law to Transnational Personal Data: Trends and Dynamics', (2020) German Law Journal 1285.

## VII. Decentralised governance structures

Decentralised governance within distributed platforms may be managed by a community of members who have the right to propose initiatives through DAOs.[106] In order to pursue a purpose with minimal human intervention,[107] DAOs use coded smart contracts to set out the rules for what the purpose of the DAO is, how members agree to cooperate, how decisions are collectively taken through a voting process, how native tokens are created and distributed, and how transactions are executed once certain triggering conditions are met.[108]

A DAO is therefore a tool to achieve decentralised governance within DLT platforms, building community management features that include the pooling of tokens, voting, audits and multisignature wallets.[109] A DAO may have the potential to be characterised as a trust form, or at least to use the trust form as the closest analogy that may limit the liability of DAO members in the absence of a corporate form.[110] Trusts as a potential legal holding structure for assets of DAOs, as well as the legal recognition of DAOs as institutions analogous to trusts, may subject the recognition of DAOs to the mechanisms of the *Convention of 1 July 1985 on the Law Applicable to Trusts and on their Recognition* (HCCH Trusts Convention).[111] This may provide a potential method of providing legal recognition of DAOs across borders,

106 Sam Gabor and Noah Walters, 'Getting DAO to Business: Decentralized Autonomous Organizations Under Canadian Insolvency Law', (2022) 20th Annual Review of Insolvency Law, 2022 CanLIIDocs 4301.

107 Robert A Schwinger, 'Blockchain law: DAOs enter the spotlight', (2022) New York LJ 1, https://www.nortonrosefulbright.com/en-us/knowledge/publications/030cbf64/blockchain-law-daos-enter-the-spotlight, accessed 15 March 2024.

108 Robert Dobbyn, Rupert Morris and Marcel Treurnicht, 'Bridging the Gap – How Trusts Can Give DAOs a Foothold in the Traditional Economy', (18 March 2022), https://www.walkersglobal.com/index.php/publications/100-article/2947-bridging-the-gap-how-trusts-can-give-daos-a-foothold-in-the-traditional-economy?utm_source=mondaq&utm_medium=syndication&utm_term=Technology&utm_content=articleoriginal&utm_campaign=article, accessed 15 March 2024.

109 See *supra* note 103.

110 Carla Reyes, 'If Rockefeller Were a Coder', (2019) 87 George Washington LR 379.

111 HCCH *Convention of 1 July 1985 on the Law Applicable to Trusts and on their Recognition,* https://assets.hcch.net/docs/8618ed48-e52f-4d5c-93c1-56d58a610cf5.pdf, accessed 15 March 2024. See Alfred E. von Overbeck, "Explanatory Report on the 1985 Hague Trusts Convention", in *Proceedings of the Fifteenth Session* (1984), Tome II, *Trusts - applicable law and recognition*, (Imprimerie Nationale 1985), 370-415, paras 28-29.

relying on common characteristics such as being composed of community members with a common purpose; [112] a separate fund created in a digital environment;[113] and management through distributed governance among the members of the community.[114]

### *D. Conclusion*

The concept of digital vulnerability cuts across sectors and communities, focusing on the individual or entity that finds itself at risk by virtue of the inherent characteristics of the digital platform on which they interact. In many ways, approaching the protection of these individuals and entities, as well as their rights, from a PIL perspective takes the same tack. By cutting across the plethora of applications, platforms and purposes in the digital economy, asking and addressing the PIL questions that arise in the digital habitat directly addresses and aims to resolve the challenges that arise with digital vulnerability. By addressing the questions of what (law applies), when (such law should apply), who (should hear a dispute), and how (would parties have the opportunity to choose the law or forum), steps taken to harmonise the global PIL framework in the digital economy tackle digital vulnerabilities head on, in concrete use case scenarios, and in relation to real-world situations. Answering these questions of private international law makes us all less vulnerable as natives in the digital world that we inhabit today.

112 Aaron Wright, 'The Rise of Decentralized Autonomous Organizations: Opportunities and Challenges', (2021) 4(2) Stanford Journal of Blockchain Law & Policy 152, https://stanford-jblp.pubpub.org/pub/rise-of-daos/release/1, accessed 15 March 2024, 158.

113 *Ibid*., p. 156.

114 Carlos Santana and Laura Albareda, 'Blockchain and the emergence of Decentralized Autonomous Organizations (DAOs): An integrative model and research agenda', (October 2023) *Technological Forecasting and Social Change*, Vol. 182, September 2022; E. Naudts, 'The future of DAOs in finance - in need of legal status', European Central Bank Occasional Paper No 2023/331, https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op331~a03e416045.en.pdf, accessed 15 March 2024, 8-9.