INTERNATIONAL INSTITUTE FOR THE UNIFICATION OF PRIVATE LAW
INSTITUT INTERNATIONAL POUR L'UNIFICATION DU DROIT PRIVE

EN

Exploratory Workshop
on Digital Assets and Private Law
Rome and Zoom (17 – 18 September 2020)
[13:00–17:00 (CEST)]

UNIDROIT 2021

Study LXXXII – W.G.1 – Doc. 3

Original: English
March 2021

SUMMARY REPORT

1. On 17-18 September 2020, UNIDROIT hosted an Exploratory Workshop on Digital Assets and Private Law at its headquarters in Rome and online via Zoom. 127 participants registered for the Workshop (for a list of registered participants see **Annex 2**).

2. *Mr Ignacio Tirado* (Secretary-General of UNIDROIT) opened the Workshop and welcomed all the participants. He explained the background of UNIDROIT's work on digital assets and private law, which had originated from a broader proposal for work in the area of Artificial Intelligence, Smart Contracts, and Distributed Ledger Technology to be conducted alongside UNCITRAL. Following two jointly organised workshops in Rome (May 2019) and Vienna (March 2020), the UNIDROIT Governing Council had requested the Secretariat to narrow down the scope of this project. It was subsequently decided that UNCITRAL and UNIDROIT would continue to work jointly on preparing a taxonomy of terms in the area of the digital economy, while at the same time continue to individually work on specific areas within this domain. For UNIDROIT, it was determined that work was best suited in the area of digital assets and private law. This subject was further deliberated by an Exploratory Working Group which had prepared a preliminary list of issues which the project could potentially encompass. The Workshop was designed to shed light on these issues and discuss other relevant topics in this area in order to inform the UNIDROIT Governing Council at its 99th Session of a more precise scope of the Project. The Secretary-General noted the high speed at which the technology in this area was developing. Accordingly, UNIDROIT intended to conduct a conceptual analysis, neutral as to technology in so far as possible, in order to identify baseline rules and principles which applied to private law issues within this area.

3. The Workshop consisted of four thematic sessions chaired by Ms Louise Gullifer, Mr Marek Dubovec, Ms Nina Luisa-Siedler, and Mr Charles Mooney Jr, and a concluding session chaired by Mr Hideki Kanda, who was also the Chair of the Exploratory Working Group. (The full agenda for the Workshop can be found at **Annex 1**.)

Session 1 – Digital Assets: A Legal Taxonomy and Challenges to Private Law

4. This session considered some of the more fundamental challenges regarding the application of private law concepts to digital assets, including the application of property law concepts, the difficulties in developing a legal taxonomy of digital assets, and the challenges in mapping private law concepts onto assets based on new and ever-developing technologies. The session was chaired by Ms Louise Gullifer (University of Cambridge) and featured presentations by Mr Jason Grant Allen

(Humboldt University), Mr Tetsuo Morishita (Sophia University), and Mr David Fox (University of Edinburgh).

5. *Ms Gullifer* highlighted the importance of work in this area by noting the increasing relevance of the digital manifestation of value in the modern economy. She noted that many jurisdictions had already begun developing definitions and rules to adequately govern transactions in the digital economy. Private law issues, such as those relating to property law and third-party rights, raised in connection with digital assets were an especially important area which required close examination in order to provide greater certainty for market participants. She emphasised that harmonisation of private law rules would promote greater cross-border transactions by avoiding fragmentation and allowing parties to contract with greater confidence. While digital assets presented certain unique features and challenges, many existing private law doctrines could continue to find application. In this regard, she noted the following three possible scenarios: 1) where existing rules and principles could be applied fully to digital assets; 2) where existing rules and principles could be adapted to apply to digital assets; and 3) where new rules and principles needed to be developed. The session, and the workshop in general, sought to identify the issues which UNIDROIT's work in this area should consider addressing. She further noted that there was an important challenge in discussions in this area which she characterised as a conceptual language barrier due to the lack of a commonly agreed terminology within the digital assets sphere, reflecting the vastly different concepts and vocabularies employed by experts from the technological, economic, and legal spheres.

'The challenges presented by the question of whether digital assets are property' – Tetsuo Morishita

6. *Mr Morishita* explored property law issues arising in connection with digital assets, focusing on a number of key events related to crypto-assets in Japan which led to the development and introduction of new rules to regulate this area (i.e., Payment Services Act and Financial Instruments and Exchange Act). He proposed a distinction between two types of digital assets: 1) assets such as Bitcoin and other digital tokens which did not represent or link to anything beyond the digital asset itself; and 2), assets which represented real-world property or claims, including security tokens (e.g., representing tradable financial assets such as shares, bonds, rights in investment contracts) and tokens representing claims or rights in real or movable properties. He noted that Japanese law made a clear distinction between property rights and personal rights, whereby property rights only existed in 'things' (defined as tangible objects according to Article 85 of the Civil Code of Japan). As such, it was difficult to apply property rights and property law rules to digital assets in the Japanese context.

7. With regard to the rights of holders of Bitcoin in Japan, Mr Morishita noted that there were three distinct views on the matter: 1) that holders had no legal rights and only had *de facto* status as Bitcoin represented neither a claim nor property; 2) that a holder of Bitcoin had a property right or a similar right; and 3) that the rights of relevant parties should be determined based on the consent of network participants. He supported the second view, noting that the holder of Bitcoin could have a property (or similar) right as holders and transactors of Bitcoin could be identified through the programs within which it was being exchanged. However, different types of property law rules existed, including those for money, securities, and movable properties, and the types of rules which should apply could depend upon the nature of the transaction being examined.

8. He further noted there were indirect and direct holders of Bitcoin. (This would be discussed further in Session 3 of the Workshop). The legal meaning of the blockchain record was another important subject of debate in Japan, with a number of different possible analyses: 1) that the record was evidence of who was the owner or property right holder and whether the right was transferred from one party to another; 2) that it constituted a conclusive determination of those facts (i.e., incontrovertible evidence); or 3) that a debtor who paid a person recorded as owner on the blockchain record was discharged of his or her obligation to pay. Another possible analysis was that the blockchain record was tantamount to a 'book-entry' under the Japanese Act on Book Entry Transfer of Corporate Bond and Shares. The determination depended upon the type of digital assets

on a particular blockchain. He also noted that the legal nature of digital assets (i.e., determining whether there could be a property right or similar right in a digital asset) impacted the legal nature of contracts relating to them, and cited relevant examples including bankruptcy, transfer of assets, hard forks, security interests, attachments, theft/unauthorised transfer, and issues of private international law.

9. With regard to bankruptcy, Mr Morishita examined the Mt. Gox case to identify the rights of customers who deposited virtual currencies in digital exchanges which had later become bankrupt. In this case, the Tokyo District Court held that customers were not entitled to Bitcoin they had deposited since they were not deemed to own them, as under Japanese law, 'ownership' could only exist in assets which were tangible and subject to exclusive control. This judgment did not explore the legal nature of Bitcoin itself or its return based on other grounds. Another case relating to the same bankruptcy was filed on the basis of a trust relationship between the exchange and the customer, however, this case was settled out of court. The Amended Payment Services Act of 2019, enacted since the Mt. Gox decision, stipulated that customers who had entered into contracts for the management of crypto-assets with a crypto-asset exchange (custodian) had priority, in relation to assets segregated for customers by the exchange, over other creditors of the exchange. However, this Act did not specify the legal nature of the right which a customer had over a crypto-asset, nor the legal nature of digital assets themselves.

10. With regard to the transfer of digital assets, in Japan, the Payment Services Act and Financial Instruments and Exchange Act was amended so that, in principle, the same rules which applied to bonds and stocks also applied to security tokens. This amendment was made on the grounds that blockchains provided security tokens a degree of liquidity comparable to that of shares and bonds. However, the amendment did not provide clarity on a number of other private law issues, such as how parties could satisfy the perfection requirements for the transfers of digital assets such as security tokens. He noted that the question of what kind of perfection requirement should be applied to security tokens was the subject of extensive debate in Japan. With regard to hard forks (i.e., a situation in which a single, original digital asset is split into two new digital assets), Mr Morishita noted that a recent Japanese court decision had applied a contract law approach rather than a property law approach, concluding that there was no agreement between the customer and the exchange as to whether the exchange had a duty to provide the customer with new coins created as a result of a hard fork. With regard to attachment of digital assets, this presented difficult questions as the legal nature of a digital asset remained unclear. Attachment by third parties was unfeasible, since it depended upon the third party having the secret keys, which would rarely be the case. Lastly, with regard to theft and unauthorised transfer of digital assets, Mr Morishita noted that there was a lack of clarity with regard to the rights of persons who had digital assets stolen from them, or had their digital assets transferred without authorisation. Additionally, whether a bona fide purchaser of stolen digital assets or digital assets transferred without authorisation was protected against the competing claim of the owner was another important matter which required further consideration.

'Digitised Assets: A Legal Taxonomy and Challenges to Private Law' – David Fox

11. In the next presentation, *Mr Fox* examined how transactions involving items of digital data (in this report called 'digital assets') could be analysed as having a significance that private law recognised, primarily by mapping digital transactions on to the limited range of transactional forms currently recognised in private law. He noted that a change in digital facts did not necessarily have any effect in law, in the same way as a transaction in a real-world asset carried out in a legally ineffective manner would be a nullity.

12. Since digital assets form the basic units of digital transacting, the fundamental question was whether private law recognised such assets as patrimonial assets, or as things which were the subject of real rights (or proprietary interests in common law), as these were transactional units recognised by all systems of private law. Mr Fox noted that digital assets shared many of the general

characteristics of other assets currently recognised as property. This included their ability to be specifically individuated and exclusively controlled. Additionally, transactions with digital assets often also took place on a publicly discoverable ledger. Nevertheless, the problem of mapping digital assets onto existing notions of patrimony or things continued to exist, especially since they were incorporeal but might not represent a right to performance of an obligation owed by another party, but merely had value by virtue of the willingness of people to accept them in exchange for other things of value. In this regard, these types of digital assets fell into the category of things that many systems would only accept if they were corporeal.

13. On the assumption that digital assets could be considered to have status in property law, Mr Fox considered the mechanisms through which rights in such assets would pass from one person to another. In the case where the ledger which recorded digital transactions was legally inert, and simply consisted of a statement of digital facts, he noted that the online ledger could not operate as a legally constituted record of title, such as a land register. This was because transferability of rights through registration in legally constituted registers was rooted in the legal recognition of such a registration, whereas digital ledgers did not possess such recognition, as they were purely private arrangements, and had no backing by the law. As such, legal realities were not changed by the mere use of a ledger. Ledger transactions could only have legal effect if default rules of private law recognised the legal significance of the parties' dealings. These rules would need to be found in existing codes, statutes, or in common law principles, therefore making transactions on a ledger into expressions of the parties' intention to transact in forms which would otherwise exist in default private law. In this regard, Mr Fox concluded that such a ledger could only be secondary evidence of the parties' title, or rights to assets, and this evidence may not always be in sync with the private law recognised title of rights within the same assets, as the records on a ledger – while compliant with the internal rules of the system – might not have been compliant with private law requirements for a transfer, as in the case of theft or unauthorised transfer of a digital asset.

14. Next, Mr Fox examined the question of how rights in digital assets passed from a transferor to a transferee. To call an event a "transfer" implied that the asset in question remained the same at all stages, and that the transferee's right in the asset derived from the right of the transferor. Such characteristics did not exist in the transfer of a digital asset, as, when transferred, an asset was removed from one digital holding, and generated as a new asset in another digital holding. Such a transfer resembled a specification in property law. As such, the transferee's right was acquired through the creation of a new digital asset and could be regarded, in property law, as a version of original acquisition. This type of understanding might be thought to overcome the synchronisation problems mentioned earlier. However, some private law systems applied rules of reduction or proprietary tracing to digital assets, allowing voidable and unauthorised transactions to be challengeable. This implied that problems of synchronisation of the state of the ledger with the state of the parties' legal rights to the assets remained. Mr Fox concluded by noting that the large variety of legal forms which digital assets could take also presented a significant number of other issues worthy of further consideration, and that a singular approach to address all of them was not suitable.

'Towards a Private Law Taxonomy of "Digital Assets" – Jason Grant Allen

15. The session further examined how to classify digital assets from a private law point of view, in order to work towards a private taxonomy of digital assets. *Mr Allen* highlighted the range of digital assets which existed – including items such as game objects, e-books, digital securities, databases, digital images, DLT tokens, emails, social media data, etc. It was important to classify all types of digital assets into different well-defined categories, as well as the relationships these categories had with each other. He noted a preference for an overall structure whereby different types of assets made up subsets of the larger digital asset ecosystem. The taxonomy to be produced by UNIDROIT's work in this area needed to be an ontological database, taking into account legal realities as well as digital facts. He underscored the importance of adopting a functional approach and a technologically

neutral perspective in undertaking this work, while at the same time ensuring that relevant applicable legal doctrines were adequately considered.

16. Mr Allen noted that several existing tripartite taxonomies of DLT-based tokens had a clear regulatory focus and queried whether these taxonomies captured all of the features relevant to property law. He noted that it would be important to consider elements relating to private property law, such as ownership, transfer and encumbrance, and emphasised the role played by property rights as building blocks of private law, given that they are instrumental in allowing legal actors to shape their economic lives. Whether digital assets could be deemed as objects of property was therefore an important consideration.

17. He noted that most legal systems offered different rules for tangible and intangible objects, with some legal systems not recognising intangible objects as the subject of property rights. Legal systems also worked with a positive-negative binary approach which distinguished between fixed categories such as real and personal property (with anything not being real property being personal property), or moveable and immovable property (where anything which was not immovable was moveable). These types of approaches failed to align with the technical and legal realities towards which digital asset taxonomies pointed and had resulted in domestic civil law legislations trying to incorporate digital assets into traditional legal theories and conceptualisations.

18. English property law could be fairly accommodating towards intangibles objects, which fitted within the categories of incorporeal hereditaments (real property), and choses in action (personal property) which could be divided into documentary intangibles (sometimes similar to choses in possession) and pure intangibles. Mr. Allen noted the usefulness of a generic property law-based taxonomy for intangible assets in the digital economy, as they formed a major part of this global economic infrastructure. He noted that most legal systems had mechanisms to accommodate rights within incorporeal objects which they treated as things. These could be used to accommodate certain categories of digital assets, despite leaving open existing problems with such treatment of objects. With objects such as Bitcoin, the problems were exacerbated. Several types of digital assets and data were potentially difficult to classify. One type was assets, such as Bitcoin, which were not rights against a person or in a thing. Another type covered rights which were documented digitally and which were not (necessarily) "documents of title" or "negotiable instruments". Specific care needed to be given to internal definitions within a category of digital assets, such as distinguishing between DLT based digital bonds and other digital bonds, keeping in mind the absence of a document in the former. Additionally, certain categories would likely need to be excluded, such as game objects and .mp3 files.

19. In concluding, Mr Allen noted there were fundamental questions which should be considered at the outset, including: why value was ascribed to digital objects; the properties of those digital objects which made it possible to ascribe them value; the processes through which digital objects of value were created; the role of documentation; and the significance of the increasingly dynamic nature of documentation.

20. A participant queried to which extent an understanding of the technological background at a granular level was required before undertaking a private law analysis. For example, where a transfer took place through a consent mechanism such as a blockchain, only a probability of certainty existed at the moment the transfer occurred and one block was created, with certainty only attained when a certain number of subsequent blocks had been created across the blockchain, thereby confirming the transfer. As such, technological traits of specific digital assets could contradict private law doctrines and should be understood prior to the development of rules in this area. The panellists noted that uncertainty in the factual granularity of transactions existed even in real-world assets, upon which conclusions of a legal reality had to be vested. The panellists noted that private law rules needed to be technologically neutral and as such, a specific understanding of granular aspects of

technologies relating to particular types of digital assets would not always be practicable or necessary (especially in a technological environment that was constantly changing).

21. A participant noted that existing rules on property were not technology neutral, as they had been developed on the basis of technologies such as paper-based documents or face-to-face transactions. It was noted that identifying functional equivalents between new technologies and older ones, while at the same time remaining technologically neutral in relation to new technologies, might not be pragmatically possible. Another participant concurred with the need to have an understanding of the technologies before developing legal rules in relation, for example, to transfers or transmissions. Another participant noted the usefulness of analogies in enabling a better understanding of digital assets. Additionally, work done as part of the UNCITRAL Model Law on Electronic Transferable Records regarding control and singularity of assets could be useful in developing functional equivalents between digital assets and real-world assets. It was also noted that language related issues, including those involved in translation into different languages, would also be challenging in undertaking this work.

22. A participant noted that UNIDROIT's work in this area had stemmed from a broader proposal by the Government of the Czech Republic in 2016. It was noted that the work on preparing a taxonomy required input from experts in technology, as well as legal experts from both a common law and a civil law background. It was important to examine the definition of a digital asset, and to determine the types (with examples) of digital assets which UNIDROIT's project would cover. Additionally, terms such as ownership, control, and possession of digital assets would also need to be elaborated. The panellists concurred regarding the importance of the elaboration of these terms.

23. A participant noted that digital assets were not intangible, but in fact physical (albeit on a very small scale). Treating digital assets as physical property could allow legislators to rely on the existing public and private law rules available for tangible assets and develop reform much more smoothly. Additionally, during a transfer of a digital asset, only some technologies had a mechanism where the asset was destroyed on one end and a new asset created on another. As such, a technology neutral approach should be consistently adopted in developing rules in this area.

24. A participant noted that legal theories of intellectual property law were relevant for examining rights in intangible assets, and that IP law concepts could be useful to consider as part of this project. The panellists concurred with the relevance of intellectual property law for work in the area of digital assets.

25. A participant noted that the Law Commission of England and Wales had started a project examining the legal status of digitised assets. This project also considered the nature of digitised assets and was to consider the possibility that they could be treated in private law in the same way as tangibles. It was noted that the Law Commission of England and Wales welcomed input from the participants at the Exploratory Workshop on their work.

26. The panellists reiterated the importance of technological neutrality in order to ensure the broader applicability of legal rules to technological developments and advancements. The technologically dependent status of existing legal rules (designed for the physical world, paper-based documents or face-to-face transactions) was acknowledged, and it was noted that treating digital assets in the same way as tangibles could resolve a number of issues relating to the distinction between possession and control of a digital asset. Digital data sometimes only served as evidence of the existence of an off-ledger digital asset, rather than the asset itself – as such, the variety of digital assets in circulation would need to be considered in making an assessment of their corporeal or incorporeal nature. The panellists agreed on the importance of having an understanding of the technology when developing legal rules. They further noted that additional consideration needed to be given to the tangible or intangible nature of digital assets. An analogy was drawn between nodes containing digital data which comprised a digital asset, and, on a physiological level, the neurological

chemicals which comprised human thoughts, noting that care had to be taken in extending the corporeality of different types of objects. Tangibility should be considered in a legal sense, rather than a factual one.

27. In concluding the session, it was noted that technological specificities would always be examined at the court level, as any court considering the application of legal principles to a case had to consider the facts of the case in order to render a decision. Additional deliberations were needed to ascertain the nature of digital assets, as well as to further understand the applicability of doctrines such as ownership, possession, and control over such assets. Various jurisdictions applied these doctrines in different ways, and the project would endeavour to explore these in detail.

Session 2 – Legal Issues in the Use of Digital Assets as Collateral: Existing and Emerging International Standards

28. This session discussed a number of legal issues surrounding the use of digital assets as collateral for loans. It provided illustrations of typical transactions and examined how the existing and emerging international standards, including the UNCITRAL Model Law on Secured Transactions (UNCITRAL MLST) and the ALI-ELI Principles for a Data Economy, addressed legal issues that arose in the context of secured transactions and could be applied to the use of digital assets as collateral. The session also identified the aspects of secured transactions that UNIDROIT's project on digital assets would explore in coordination with these standards. This session was chaired by Mr Marek Dubovec (Kozolchyk National Law Center) and featured presentations by Mr Andrew Hinkes (Carlton Fields), Mr Steve Weise (Proskauer Rose LLP), and Ms Teresa Rodríguez de las Heras Ballell (Universidad Carlos III de Madrid). It was noted that a discussion on digital assets also had relevance for a number of other projects which made up UNIDROIT's 2020-2022 Work Programme, including a Model Law on Factoring, a Model Law on Warehouse Receipts, as well as the project focussing on Effective Enforcement.

'"Collateralized" transactions using DLT-derived assets' – Andrew Hinkes

29. *Mr Hinkes* provided examples of digital assets which were used as collateral, as well as different types of transactions with digital assets which feature an element of financing. He also examined new types of DLT-based assets which emulated structures of secured transactions without satisfying the applicable legal requirements.

30. Mr Hinkes provided an example of a fiat money loan to a borrower who provided Bitcoin as collateral, whereby the fiat moved from the lender to the borrower pursuant to a loan agreement. In this instance, the applicable method of perfection would be to file a financing statement because Bitcoin would not fit under specific types of collateral under Article 8 or 9 of the UCC. As such, the rules governing general intangibles would be applicable. Perfection by registration would not normally be used for the purpose of exercising legal rights as to the collateral, but rather to establish priority in case of bankruptcy of the borrower. Some lenders also use securities intermediaries to enable the perfection of their security interests through acquiring control that also confers super-priority i.e., priority even over an earlier-in-time registration.

31. It was noted that lenders use structures such as multiple signature wallets in conjunction with legally enforceable agreements to exercise control over collateral such as Bitcoin. These constructions rely solely upon wallet technology where digital assets are held. When held in a multi-signature wallet, a transaction must be authorised by a specified number of private keys required for that wallet, with each being held by a different person. Third parties who hold a private key have contractual obligations for when they could use their keys (making the third party similar to an escrow agent). In case of a default, following notice and opportunity to cure it, the lender and the

third party could use their keys to transfer the digital asset, for instance, under the sole control of the lender.

32. Many of these lending structures often depended upon the value of the collateral, which could fluctuate, resulting in notice and cure periods for defaults being very short. This could result in issues of applying commercial reasonableness in the context of expeditious enforcement when mapping existing rules onto such transactions. Mr Hinkes noted that most of these transactions were one-way, such that there was no mechanism to return assets which had been transferred from wallet to wallet.

33. Mr Hinkes drew attention to smart contracts, a mechanism which automatically enforced an agreement which had its terms captured in computer code. In the context of digital assets, a smart contract was a wallet in a blockchain system that could hold and transact digital assets based upon the execution of its code logic. He described smart contracts built on top of blockchain infrastructure, such as the system of Ethereum, which involved a code deployer putting smart contract code on a digital wallet which was available for use by the public. Digital assets could be placed within this wallet, which would automatically function on the basis of data (referred to as an oracle), all of which was already described in the smart contract code. Following the input of specific types of data, agreed changes/transactions could take place to the digital asset held within the wallet subject to the smart contract code. No interference was possible in the execution of the smart contract code, which was fixed once deployed. The type of activities possible within a smart contract were limited by the code. Smart contracts were purely mechanical in nature and agnostic to court orders, pleas of parties, etc.

34. He also described the operation of a MakerDao vault (a Maker Protocol Smart Contract Modules System), a popular DeFi (decentralised finance) product. The MakerDao vault provided a party with the ability to engage in leveraged retail commodity transactions. Through the use of smart contracts and blockchain, it emulated financial transactions which would traditionally involve counterparts who rely upon trust. A simplified 'creation' transaction in MakerDao entailed a funder depositing Ethereum or other collateral into a 'vault' CDP (Collateralised Debt Position) smart contract. The vault then sent a message to another smart contract, a 'DaiJoin', then making available to the funder a new asset (DAI), which was another instrument created by the MakerDao system – in this case, a price stable asset pegged to USD (1 USD = 1 DAI). The amount of DAI made available was dependent upon the amount of collateral deposited in the vault. The ratio of DAI to Ethereum collateral in the system was fixed. Vaults were freely transferable, which meant that interests in vaults could be provided to other parties. Such systems were used by individuals with assets who 1) preferred to borrow against them rather than sell them to avoid tax obligations; 2) were not confident in the value of their collateral; or 3) interested in leveraging their collateral exposure. It was noted that the system was designed to be over-collateralised, meaning that it did not provide loans or extend credit because the system always required more collateral to be provided, as compared to value derived out of it. He noted that liquidation in a vault could be triggered at the right liquidation ratio when the value of the collateral dropped below a certain point relative to the value of the DAI that had been removed. In a liquidation the vault was closed, meaning that the control over that vault was transferred from the owner to a liquidity providing smart contract, to determine the amount of collateral needed to be sold to restore the ratio. A centralised DAI dashboard allowed participants to bid on the collateral being sold with DAI. The DAI used to buy the collateral was burned in order to restore the balance. The remaining collateral was provided back to the vault. The purchasers were provided a discount in acquiring market collateral, which was adjusted in different places within the system. Liquidation only took place where system participants noticed a vault not adhering to the liquation ratio. As such, this entire system depended upon the smooth functioning of smart contracts, as well as a number of other technologies – noting the system also presented vulnerabilities relating to functionality (e.g., software vulnerabilities, high congestion due to bandwidth limitations, etc.).

35. Mr Hinkes concluded by noting the types of digital assets frequently used as collateral. These included crypto-currencies such as Bitcoin and Ethereum, as well as DLT-native stablecoins (such as USDC and GUSD), ERC20-based instruments, and smart contract-generated DLT native digital assets (such as DAI). Less frequently used digital assets included their derivatives such as Wrapped Bitcoin or Wrapped Ethereum, and algorithmically stabilised DLT natives such as Based, as well as digital asset securities, non-fungible tokens, and DLT instruments backed by real world assets.

'Security rights in data and Smart Contracts – Steve Weise

36. *Mr Weise* examined common language used in various projects in the digital assets space, including those carried out under the auspices of organisations such as the American Law Institute (ALI), the European Law Institute (ELI), and UNCITRAL. He examined the importance of and the need for predictability and legal certainty in transactions of digital assets, particularly of a cross-border nature, and noted the need for common harmonised approaches, definitions and forms to be used in such transactions. He illustrated the various issues in secured transactions involving digital assets as well as the challenges associated with resolving them, and highlighted the global, European, and American efforts underway to address them. These challenges included issues of language, applicability of terms and definitions across systems and jurisdictions, translation of terms, as well as horizontal and vertical issues of consistency of concepts. He highlighted different approaches across jurisdictions with regard to terms such as possession and property, and pointed out that various terminologies presented issues, including those such as possession and control, tangible and intangible asset, which all received differing treatment across jurisdictions.

37. The question of whether digital assets could be considered to be amenable to property rights was examined further. Within legal systems, words could have variable meanings. Mr Weise noted that in some legal systems, rights under a contract rather than obligations under a contract could be treated as a property, and, as such, be capable of having security rights over them. From a global perspective, he noted that significant work has been undertaken insofar as incorporating digital assets within the UNCITRAL MLST, with other organisations also working towards developing instruments in this area. He highlighted the value a global taxonomy of terms could provide, noting that UNCITRAL and UNIDROIT were well positioned to prepare one. Harmonisation of work in this area should enhance certainty and predictability. He also noted the work done by the Hague Conference on Private International Law on the law applicable to certain rights in respect of securities held with an intermediary and its possible influence on the law applicable to transactions with digital assets.

38. From amongst the regional initiatives, Mr Weise highlighted the European Union Financial Collateral Directive, which did not specifically cover digital assets, but could be examined as a draft common frame of reference. The United Kingdom's legal statement on crypto-assets and smart contracts was also a useful document to explore further. This study concluded that nothing prevented data from being recognized as property, and nothing prevented a smart contract from being a contract, under the laws of the United Kingdom. The European Law Institute and the American Law Institute have been working on a joint project called the Principles for a Data Economy, which examined transactions in data and characteristics of data, without addressing the question of data as property. He noted the importance of answering the question of digital data as property, especially in order to address other questions such as those of insolvency, secured transactions, inheritance, etc. He considered that digital assets presented sufficient characteristics of property to be subject to a property right – however, this was not globally agreed upon.

39. Mr Weise concluded by noting the laws in the United States, especially the UCC, did not contain a definition of property and left room for debate for the treatment of digital assets. There were also issues of consistency with the Bankruptcy Code which needed further examination and could benefit from harmonisation with the underlying property law. In these efforts, the question of language needed close examination, particularly in addressing issues of vertical integration within a given jurisdiction.

'Security Interests on Digital Assets: Issues to Consider' – Teresa Rodríguez de las Heras Ballell

40. *Ms Rodríguez de las Heras Ballell* examined standards and principles within the UNCITRAL MLST and queried their applicability and usefulness to secured transactions in digital assets. She identified potential gaps, and how they could be filled. She noted that the first questions to be addressed were those of terminology, concepts, and scope. The application of any sets of rules depended upon the meaning of the term 'digital assets'. In taking a broad understanding of digital assets, three possibilities emerged: 1) to treat digital assets as a new type of asset which required the adoption of new rules; 2) to treat the problem as one of legal characterisation, which could be resolved by finding functional equivalents of different digital assets with real-world assets (either tangible or intangible) – with existing rules adapted accordingly; and 3) even where existing rules applied, there would be a need to adjust and adapt mechanisms for creation, perfection, custody, delivery, and transferability of digital assets, in a legal or technological manner.

41. Ms Rodríguez de las Heras Ballell further elaborated on effectiveness against third parties (perfection), priority, enforcement, and conflict of law. She outlined the applicability of rules in these areas in the UNCITRAL MLST to digital assets as a testing exercise to assess the adaptability of existing rules to digital assets. Regarding effectiveness against third parties, the primary methods in the MLST were registration and possession (for tangible assets). The MLST also included asset-specific rules that allowed for consideration of other methods such as control agreements, designation as bank account holders, possession of negotiable documents, book entries with respect to non-intermediated securities, etc. As such, the question of whether digital assets were tangible assets or intangible assets needed consideration. Any analysis of the applicability of the rules would need a characterisation along these lines for the digital assets in question, after which the perfection rules could apply accordingly. At the same time, methods for taking possession and control over digital assets also needed to be considered, including legal issues, practical considerations, and technological aspects related to private keys.

42. With regard to priority rules, the UNCITRAL MLST provided for general temporal rules according to the order of third-party effectiveness or the time of registration, as well as asset-specific non-temporal rules. With digital assets, applicable priority rules would depend upon the prior legal classification of a digital asset. Additionally, there might be practical difficulties for the secured creditor to locate and trace transferees of digital assets when the security right had not been extinguished. Additionally, the question of whether control for the perfection of security rights in digital assets should be recognized needed further consideration. Determination of the priority of secured creditors, in an anonymous system such as in distributed ledger systems, was also problematic, and new rules might be needed.

43. With regard to enforcement, she noted that the UNCITRAL MLST provided the option to exercise rights by applying to a court, or to exercise rights extra-judicially. For enforcement of security rights in digital assets, the concept of providing notice to competing claimants was inconsistent with the market practice of instantaneous transactions. Additionally, irreversibility of certain actions in DLT systems as well as the lack of traceability led to several additional issues in enforcement. It was also noted that transfers of private keys were not registered in the ledger, adding complexities and enabling untraceable actions within the DLT system. She also highlighted the issues presented by smart contracts for pre-programmed enforcement which were not aligned with mechanisms found within the UNCITRAL MLST and might not meet the applicable requirements.

44. With regard to conflict of law rules, she highlighted that the UNCITRAL MLST determined the application of law according to the location of the asset (for tangible assets), the location of the grantor (for intangible assets), but also contained some asset-specific rules. When examining digital assets in this context, location was a difficult concept to transpose. Relevance of keyholders' location could be considered, as well as the location of the nodes. The nature of a wallet provider as a deposit-taking entity could also be explored.

45. In conclusion, she noted that without identifying the nature of digital assets, it was not possible to analyse the applicability of existing rules to these assets.

46. A participant noted the similarities between certain transactions which were highlighted by Mr Hinkes and a title transfer collateral arrangement under English law, which was largely enforced by netting. This was not a secured transaction. Another participant queried the global acceptance of assets such as DAI as collateral for the purposes of a secured transaction, noting their volatility. The panellists noted that the lack of clearly discernible counterparties in such transactions (as funders were often interacting directly with computer code) made it difficult for netting principles to apply, which required counterparties. This problem could be resolved by considering the system provider as a counterparty, or by trying to identify real counterparties behind such transactions. In the case of MakerDao, transactions occurred between funders and smart contracts, whereby the smart contracts did not require any human input to operate. However, the operation of the system had to be manually determined (including items such as assigning a liquidation ratio). Moreover, individuals who held them exercised governance tokens within these systems which also determined the way transactions took place. As such, while smart contracts did not have identifiable counterparties, individuals with governance tokens determined parts of the operation of the system as a whole.

47. A participant queried why there was a need to characterise the collateral transaction as either a security interest or a title transfer involving the asset as subject to security or title transfer. Instead, a person might take cover for an exposure by getting a standby letter of credit from a third-party bank/obligor of good credit standing whereby upon default, the person could trigger the letter of credit and get paid out from the proceeds.

48. A participant expressed concern with the large number of organisations involved in law reform for electronic commerce. The importance of uniformity was stressed, and it was noted that UNIDROIT and UNCITRAL could bring together these various initiatives to produce a uniform instrument. The participant also queried the relevance of preparing such an instrument, as the larger goal could be to enable a system that governed itself and did not require enforcement by institutions. Another participant noted that digital assets had created several new asset classes, which would require new asset specific rules that might need to be incorporated within instruments such as the UNCITRAL MLST.

49. The panellists noted that further consideration would need to be given to the extent to which a system could be self-regulated, while noting that the structure and source of the systems would still need to be anchored in the law. The panel noted the relevance of drawing analogies with existing types of assets in developing new rules for digital assets. The panel also stressed the importance of harmonisation of rules in this area.

Session 3 – Digital Assets Linked to Real-World Assets (Digital Twins): Civil Law and Private International Law Implications

50. This session focused on exploring the issues of 'digital twins' which represented a real-world asset and typically faced problems of how to prevent the digital twin from separating from the real-world asset which it represented. The speakers explained how their respective jurisdictions dealt with these issues. They also shared their practical experience with the multi-jurisdiction issues faced by many, if not all, digital asset projects, stemming from the fact that in most cases more than one jurisdiction was claiming to be applicable to the digital asset. This session was chaired by Ms Nina-Luisa Siedler (DWF Germany) and featured presentations by Mr Thomas Nägele (NÄGELE Attorneys), Ms Joshua Klayman (Linklaters), and Ms Urszula McCormack (King & Wood Mallesons).

'Bridging the Real World with Virtual Assets' – Urszula McCormack

51. *Ms McCormack* noted that digital twins referred to digital counterparts of real-world assets of any nature. Whereas some of the private law issues concerning digital versions of real-world assets reflected the same issues linked with the real-world assets themselves, and were thus not new issues per se, others presented new challenges. She examined the legal aspects of tokenising real-world assets, noting that several types of risks arose at multiple stages of the asset life cycle. These covered a wide range of issues relating to: the asset's ideation and creation, its existence, its authenticity, ownership of the asset, its provenance, its inherent properties, its quality, its function, custody issues, its transferability, activities, and end of life. She noted that tokenisation of assets involved the digital representation of real (physical) assets on distributed ledgers, or the issuance of traditional asset classes in tokenised forms. This was not a new concept and was simply a mechanism to record certain rights and interests within an asset.

52. While private law issues existed throughout the life cycle of an asset, issues of existence of the asset were important to examine in the context of tokenisation, such that the tokenised asset accurately represented the rights relating to the real-world asset. Additionally, issues of ownership and transferability were also relevant and closely linked, with the mechanics of transferability (of the tokenised asset, as well as the real-world asset) carrying a high degree of importance. Different jurisdictions required certain specific procedures to be carried out before the transfer was recognised by law; this typically involved some form of notice, however, the legal steps required for transfer were not necessarily the same as the steps required by the technical system in question (e.g., blockchain, etc.). She emphasised the importance of the linkage between the two (i.e., the legal and the technical requirements), noting there was sometimes a lag in time between the technical transfer and the legally recognised transfer. She noted there were two core systems available for ensuring that an asset and its representative instrument remained linked: the first was a register and the second was control. Ms McCormack added that the inherent properties of the tokenised asset needed to be examined, and issues of custody and the activities which could be undertaken with a tokenised asset were important to analyse further.

53. Ms McCormack highlighted some examples of tokenised assets and the issues which they raised. She noted that company shares were a type of asset suitable for tokenisation, however, many jurisdictions had highly prescriptive measures for the registration of company shares, including matters such as location and types of registers. Moreover, requirements for paper-based processes (such as stamp duty) also made tokenisation and transfers of tokenised company shares cumbersome and led to parties using processes whereby the legal transfer of a tokenised asset only took place sometime after the procedural transfer on a blockchain. She noted real estate as another example – real estate could be fractionalised which made it a good candidate for tokenisation. However, title systems which relied on physical registers and paper-based documents made such transfers using tokenised real estate difficult. This was addressed through the creation of funds which were more flexible, and were recorded as a collective investment, rather than individuals having interests in particular assets.

54. She noted soft commodities (e.g., merino wool) as another example of assets which could be tokenised, and which were of a fungible nature, pointing to the important issues of authenticity and quality inherent in this process. Additionally, non-fungible individual assets (e.g., diamonds) could also be tokenised which raised questions of provenance, as well as compatibility with already existing registers. She also highlighted special assets such as space assets and aviation assets which often had special requirements under domestic or international law (noting the example of registration requirements in space assets which originated from the 1975 Convention on Registration of Objects Launched into Outer Space).

55. Ms McCormack concluded by highlighting some of the key considerations relating to and challenges posed by digital twins, including questions regarding: the components of underlying assets; their inherent divisibility/fractionalisation potential; contextual considerations; jurisdictional nexus factors; domestic rules relating to asset ownership, custody, transferability, and activities relating to the assets; the process and significance of tokenisation; private international law principles; the legal and contractual framework for effectuating the linkage; and vulnerabilities which could be challenged.

'The Liechtenstein Blockchain Act' – Thomas Nägele

56. *Mr Nägele* examined the blockchain regulation and comprehensive framework for digital assets adopted by Liechtenstein, a civil law jurisdiction. The Liechtenstein Blockchain Act featured 58 Pages, 51 Articles, and its Full Report was 384 pages long. It contained amendments to the Due Diligence Act (SPG), the Financial Market Supervision Act (FMAG), Corporate Law (PGR), and Trade Law (GewG). He noted that the Act defined a token as a piece of information on a Trusted Technology (TT) System which could represent claims or rights of membership against a person, rights to property, or other absolute or relative rights, and was assigned to one or more TT identifiers. TT systems were used in the legislation to reflect technological neutrality, and they referred to systems which worked without intermediaries and could be trusted by users. The main functions of tokens were legitimisation (for the benefit of the beneficiary), liberation (in favour of the debtor), and transportation (the transfer of the underlying rights).

57. The Act dealt with links between assets and tokens, as well as tokens and individuals. For the relationship between the tokens and the individuals, the Act defined 'TT keys' and 'TT identifiers'. An important aspect of the Act was the provision relating to disposal over the tokens which referred to the disposal of the rights represented by the token. The Act was intended to be used for the tokenisation of all sorts of assets by allowing tokens to be representations of rights within assets. The Act also defined new types of service providers (a type of intermediary) in this area.

58. With regard to the civil law aspects of the Act, Mr Nägele noted its use of the token container model as a term for describing a specific element of the digital token in question. This meant that the legal definition of a particular token could be found within a container with specific functions. In the example of a diamond, a token could represent the ownership right within a diamond. The technology in which tokens existed allowed for ease of transferability of tokens, which was the main advantage of using them. With regard to the physical object (i.e., the diamond itself), the transfer of an ownership right by way of the transfer of a token was an enforceable way of acquiring the physical object.

59. One of the main goals of the Act was to allow for the enforceability of digital transactions. For this, consideration had to be given to the meaning of possessing a token (under the property law regime of Liechtenstein, a physical element was necessary in order for possession to exist, and tokens were not treated as physical in nature). For this, the concept of a power of disposal (similar to possessor) was developed, which was a person with knowledge of the TT key of a token. Additionally, the concept of right of disposal (similar to an owner) was developed, who was a person entitled to use the TT key. The requirements for the process of disposal over a token included the following: that the transfer was in line with the regulations of the TT system; that the consent of the parties was obtained; and that the power of disposal of the transferee existed. There also existed provisions regarding good faith.

60. The effects of a disposal of a token were the disposal of the rights represented by that token. However, this presented certain legal challenges in assets where coordination between the transfer of the tokenised right and the physical asset was required. In order to address this, Article 7 of the Act specified that if the legal effect of the disposal did not come into force by law, the person obliged, […], must ensure through suitable measures that: a) the disposal over a token directly or indirectly

resulted in the disposal over the represented rights; and b) a competing disposal over the represented right was excluded. As such, solutions needed to be found on a case-by-case basis for different types of assets.

61. In conclusion, Mr Nägele noted that the combination of a system of trusted technologies, as well as a legal framework for transactions within them, allowed for effective enforceability of digital transactions with regard to their real-world assets in Liechtenstein. In order to bridge the gap between the physical and the digital world, to ensure enforcement, avoid conflicts of rights, and to allow for the identification and storage of real-world assets, the Act created physical validators who were people who ensured the enforcement of rights in accordance with the agreement, in terms of property law, represented in tokens on TT systems. He added that several challenges still existed: for instance, most transactions had an international scope and enforcement was only possible in Switzerland and Austria (countries with which Liechtenstein had bilateral agreements); he also noted that physical rights and incorporeal rights represented by tokens generated different types of legal complications.

62. The panel briefly discussed issues related to the establishment of applicable jurisdictions for the contractual relationship between parties, and the in-rem transfer of ownership in a token and related asset. In the case where the parties to a contract made a selection as to applicable law, a determination of the law applicable to transfers of assets within those contracts would be straightforward and respected by courts. However, where parties did not make such a selection, courts could apply a number of different types of tests to determine the applicable law, based on public policy and other considerations.

'Questions of jurisdiction in US Law concerning digital assets' – Joshua Klayman

63. *Ms Klayman* noted that when looking at transactions in digital assets, US law largely examined only the transaction itself, rather than the rights inherent in the tokens. She noted that the State of Wyoming was one of the most developed in terms of having rules for digital assets and had passed legislation which treated tokens as property. There also existed a draft bill in Wyoming which included the idea of a digital representation token. This was largely based on tokens which existed as intangible personal property, rather than securities, making this discussion relevant to the matter of digital twins.

64. The importance of freedom of contract in international trade was noted, meaning that parties could chose to specify in their contract terms which governing law or jurisdiction applied. Nevertheless, contractual terms were not always respected in the event of a legal dispute, particularly where public policy and other considerations also had a bearing on the contract under dispute. A number of examples were provided. Under certain US State laws, in order for a choice of law provision to cover tort claims, the express language must be sufficiently broad to encompass the entire relationship between the parties, and standard choice of law provisions might not be sufficiently broad, thereby leading a court to set aside their applicability to tort claims.

65. With regard to the extraterritorial application of US law, it was noted that there was a general presumption that US law only applied to conduct within the US, except if the relevant law specified explicitly that it had extraterritorial application. This presumption, based on a Supreme Court decision, was applied in all cases (most decisions on this generally involved civil law cases, rather than criminal). This presumption limited regulatory and prosecutorial powers to investigate and bring actions involving activities outside the US. In analysing whether extraterritorial application of a given statute was appropriate, the courts analysed the focus of the statute.

66. Ms Klayman cited a paragraph from the US Supreme Court decision in RJR Nabisco, Inc v. European Community, 136 S. Ct. 2090 (2016) which read: "[i]f the conduct relevant to the statute's focus occurred in the United States, then the case involves a permissible domestic application even

if other conduct occurred abroad; but if the conduct relevant to the focus of the statute occurred in a foreign country, then the case involves an impermissible extraterritorial application regardless of any other conduct that occurred in US territory." She noted that US contacts (e.g., using the US banking system) could bring into the realm of US domestic laws conduct that otherwise took place outside of the US.

67. In the digital asset context, there were multiple potentially relevant US laws which may involve extraterritorial application, some of which permitted private rights of action. Among these were the Securities Exchange Act of 1934, as amended, and associated rules, including antifraud provisions which were enforced by private actions, the SEC and the DOJ (U.S. Department of Justice); the Commodity Exchange Act, including antifraud provisions, which were enforced by private actions, and the CFTC (Commodity Futures Trading Commission) and the DOJ; the Money Laundering Control Act, which expressly permitted extraterritorial application; and the Foreign Corrupt Practices Act which also permitted extraterritorial application. She further examined the functioning of extraterritorial jurisdiction in the Money Laundering Control Act, noting that application could be determined as long as the conduct was by a US citizen, or the conduct was by a non-US citizen but occurred in part in the US. She added that physical presence in the US was not required in order for conduct to occur in part in the US. Examples of conduct in the US could be found in a Resource Guide on this Act issued by the SEC.

68. In determining when a transaction was considered to be domestic for securities, Ms Klayman noted that in the US Supreme Court decision of Morrison v. Nat'l Australia Bank, Ltd., 561 U.S. 247 (2010), it was noted that Section 10(b) of the Exchange Act applied to: (i) transactions in securities listed on domestic exchanges, and (ii) domestic transactions in other securities. A fact-specific analysis was conducted, rather than a bright-line test. Additionally, she noted that the United States Court of Appeals 2nd Circuit had applied the 'irrevocable liability test' to determine whether a securities transaction was domestic. In this regard, the test sought to determine: (i) whether the purchaser incurred irrevocable liability within the US to take and pay for a security; (ii) whether the seller incurred irrevocable liability within the US to deliver a security; or (iii) whether title to the shares (security) was passed within the US. The goal was to identify the point at which the parties obligated themselves to perform what they had agreed to perform, even if the formal performance of their agreement was to be after a lapse of time.

69. With regard to commodities, she noted that under the Commodities Exchange Act, the United States Court of Appeals 2nd Circuit had held as follows: that Section 22 (on private right of action) did not permit extraterritorial application because it was silent as to extraterritorial reach (except potentially in the case of swaps); that private suits under Section 22 "must be based on transactions occurring in the territory of the United States"; that a transaction in a commodity occurred in the US if that was the location of the "transfer of title or the point or irrevocable liability"; and that the following, among others, must be demonstrated: (i) proof of location of the transactions, including the formation of contracts, (ii) the placement of order, (iii) the passing of title, and (iv) the exchange of money.

70. Ms Klayman provided an example from an ongoing case on this matter, noting that these issues were actively being litigated. In this case, the courts had applied the irrevocable liability test and focused on the actual location of where the digital assets transactions took place. This involved examining items such as where the website for the digital asset sale was hosted, where clusters of nodes were situated when the asset sale became irrevocable, and that the plaintiff participated in the digital asset sale, presumably, because of marketing that heavily targeted US residents. She also briefly noted details about the Howey Test which applied in the context of US Federal Securities Laws.

71. A participant queried whether the Liechtenstein Blockchain Act applied to physical assets which could not be considered to be held in custody, such as real estate. It was noted that the Act did apply, however, there were mandatory rules which applied to transfer of property which entailed

practical limitations to its application. Another participant raised a query regarding the notion in the Liechtenstein Blockchain Act specifying that the transactions must align with the elements of a TT system, wondering what such elements were. Additionally, in the case where a unique object was destroyed upon transfer, how would the process of obtaining evidence to confirm that it was truly destroyed proceed in enabling enforcement. It was noted that each TT system had its own elements, and a transaction must follow the elements within each system. Additionally, for any faults within a given TT system, the system operator would be liable. With regard to evidence, proof within the system (such as a search in a blockchain explorer) could be used, with the courts accepting digital evidence of such a nature.

72. A participant queried the protections available for a bona fide third party under the Liechtenstein Blockchain Act. It was noted that Article 9 protected the acquisition of tokens in good faith, even if the selling party was not entitled to dispose of the particular token (unless the recipient party was aware, or should have been aware of the lack of right of disposal). With regard to a lack of synchronisation between the real-world asset and the tokenised asset, in terms of the position of a bona fide third party, the real-world asset's ownership would take priority. The use of real-world validators had been developed to counteract this issue. Some registries (such as the system in Australia) deemed the register as the ultimate arbiter of ownership. As such, a bona fide purchaser without notice of someone else's prior claim did not exist in such systems, as the register was treated as notice.

73. A participant queried whether the Liechtenstein Blockchain Act contemplated other mechanisms of transferring the tokenised real-world asset independently from the token. It was noted that such would depend upon the specific rules within a TT System, or the registry which was taken as evidence of a transfer. Alternatively, immobilisation of property or hindering the transfer of the right sometimes also took place. Another participant queried how the synchronisation issue would be managed if it were possible to transfer an asset off-chain. A further query concerned whether a statute was required to make the register the effective root of title, and whether or not such a statute needed provisions for rectification of the register. It was noted that the need for legislation depended upon the type of asset or right which had been tokenised, for example, in the case where a right within a fund, or any other private system, had been tokenised, the rules could be managed directly by those who managed that fund or private system; however, for assets which had a more public related right, such as rights within property, legislation would be necessary. In Liechtenstein, legislation was deemed necessary with regard to rectification, noting the technical impossibility of rectification in cases of wrongful transactions in digital assets.

74. A participant queried the responsibility/liability carried by the physical validator in Liechtenstein insofar as ensuring the correct disposal of the real-world asset to the most up-to-date token holder, or in cases of loss or destruction of the real-world asset. It was noted that Liechtenstein required physical validators to submit their plans and functioning to the financial regulator, as well as conduct a significant degree of due diligence regarding their clients and stakeholders. Additionally, insurance requirements also existed to address these issues.

Session 4 – Intermediated Digital Assets: Custody Issues

75. This session addressed the settings in which an acquirer of digital assets chooses to hold the assets through a custodian and compared "direct" holding with various structures for custodial holding. It explored the practical and legal aspects of custodial holding from the perspectives of an acquirer and a custodian, including issues of private law and insolvency law. This session was chaired by Mr Charles Mooney, Jr. (University of Pennsylvania) and featured presentations by Ms Carla L. Reyes (Southern Methodist University), Mr Matthias Haentjens (University of Leiden), and Mr Stephen A. Keen, Esq. (Perkins Coie LLP).

'Methods for Holding Digital Assets' – Carla Reyes

76. *Ms Reyes* explored methods for holding digital assets. She detailed five different options users could utilise to hold cryptocurrencies (primarily using Bitcoin as an example). For interacting directly with the blockchain protocol, the first option was to hold the cryptocurrency directly. This could be done by downloading the Bitcoin Core software which contained a wallet. This had the advantages of allowing full control over the assets, as it was a full node that validated and relayed transactions on the BTC network. Additionally, there was no need to trust third-party verification, and it offered the ability to set fees and monitor them directly. The disadvantages of this were that the individual was solely responsible for securing and backing up their wallet. Full nodes also required more storage space (over 350GB) and internet bandwidth and was ultimately only as secure as the hardware it ran on, requiring significant amounts of additional security measures. She presented a series of screenshots to illustrate how such a system operated, noting that the software needed to be synced to the blockchain, and the wallet needed to be encrypted and backed up regularly. She further noted that it was possible to create as many public and private keys within the wallet as desired. For added security, some users created a new wallet for every transaction, while other users also used their own multi-signature wallets.

77. The second option was to use a Simplified Payment Verification (SPV) wallet. Most smartphone non-custodial wallets were of this nature. These wallets checked to see if a transaction had been verified by a miner and whether the transaction showed up on the blockchain. This was more secure than internet third-party wallets as it did not need to trust third-party providers, and it allowed an individual to keep their own keys and allowed control over fees. However, in case an individual were to forget their password and seed phrase, the assets were lost forever. Additionally, it was only as secure as the hardware it ran on, which was usually a mobile device less vulnerable to malware than a computer, but easier to lose. There were also a number of scams in existence which aimed to spoof the SPV software. She again showed a number of screenshots to illustrate how such a system operated and noted its ease-of-use.

78. By using third-party non-custodial software and/or hardware, the third option to hold cryptocurrencies was to use online wallets. In this case, the interface was familiar to most users. It was important to note that the noncustodial online wallets did not have technical access to a user's private keys. However, with online wallets, a user did not have total control over their private keys, hence, if a user were to forget their password and seed phrase, the assets would be lost forever. Moreover, as the private keys were decrypted client-side, the system was still vulnerable to computer malware, and also vulnerable to attacks on software providers.

79. The fourth option was the use of a hardware wallet. These were not online unless a transaction needed to be made. These allowed a user full control over their assets and provided for a very secure environment because of the secure specialised setting provided by the device. However, in the case of loss, damage, or theft of the hardware, the assets could be lost. Additionally, payment validation, privacy, and fee control were all determined by the software wallet which a user used in connection with the hardware whenever a user wanted to make transactions.

80. Ms Reyes noted that the fifth option to hold cryptocurrencies was through the use of an exchange which was a custodial wallet provider. This provided a very user-friendly experience and sometimes even offered offline storage options. There were also tools available for account recovery. However, using an exchange involved trusting a third-party with private keys, as well as having to rely on whether the custodian had taken adequate security measures and was trustworthy. Ms Reyes stressed the importance of users taking adequate security measures by themselves to ensure the safety of their assets. She encouraged practices such as encryption, multi-signature wallets, usage of multiple types of wallets, as well as other online and offline security mechanisms.

'Client Protection in Custodian Insolvency' – Matthias Haentjens

81. *Mr Haentjens* examined client protection in case of crypto custodian insolvency. He noted that a majority of investors in cryptocurrencies presently relied on custodians. These could be exchanges, or specialised custodians which offered cryptocurrency services. In examining the terms and conditions of the largest crypto exchanges, he noted that they included two forms of custody: 1) custody in segregated form where custodians advertised to administrate crypto-assets per client, i.e., on an individual basis; and 2) an omnibus account model where the custodian administered a pool of crypto-assets held for clients collectively. The second model in particular involved a significant amount of risk, which could manifest itself in case of the custodian's insolvency.

82. Mr Haentjens noted that bankruptcy/insolvency involves significant risk when holding crypto-assets through a custodian. The legal qualification and enforcement of rights and interests in an insolvency differs from jurisdiction to jurisdiction and needed to be examined closely. He proceeded to examine legal issues that arose in some insolvencies of cryptocurrency custodians, as well as in insolvencies of regular financial institutions so as to draw lessons for cryptocustodians. He noted that in the Lehman Brothers insolvency, there were serious issues because the administration of assets was inadequate, as well as a lack of clarity as to which laws applied to them. The issues included identifying which clients held which interests, as well as which laws applied to those interests. The last category of issues was largely due to the cross-border nature of Lehman Brothers' operations.

83. In examining insolvencies of cryptocurrency custodians, Mr Haentjens noted that in the Mt. Gox insolvency in Japan, the court had decided that the relevant assets were to be considered through a contractual perspective rather than property law, which meant that the clients had a mere contractual claim against Mt. Gox. This was not beneficial to the clients seeking to recover their assets. In the Bitgrail insolvency under Italian law, the relevant assets were treated as proprietary. However, they were treated as being commingled with the custodian's own assets, which was not beneficial to the clients as it also resulted in the clients only having a contractual claim against the custodian. Most recently, in the Cryptopia insolvency in New Zealand, the relevant assets were considered as commingled with other clients' assets, but the courts assumed that a trust had come into place. A property law interest was therefore found to exist in the assets held by Cryptopia for its clients. However, the ruling also noted that there was a separate trust for every different type of cryptocurrency, which meant that in the case of a deficit in a particular type of cryptocurrency, it was only distributed amongst the clients holding interests in that specific type of cryptocurrency.

84. The key question which needed to be examined was how a shortfall would be distributed amongst clients of a crypto custodian. This could be addressed through several different mechanisms. It was noted that the assumption was that crypto investors needed to be protected. One mechanism to ensure this was to have a regulatory obligation for custodians to adequately determine which assets belonged to which clients. This would be an administrative/public law solution which aligned with general regulation of financial institutions. Such a public law solution was important, even in the presence of strong private law rules, as without proper administration of assets, private law rules have no effect.

85. It was noted that alongside a public law regulation a clear and harmonised system of private international law rules was also very important. This would need to include a harmonised idea of the nature of the claim of the investor and an appropriate, corresponding conflict of law rule. In order to do this, there would need to be a distinction between the client's claim against the insolvent estate, and the crypto-custodian's claim against the system/ledger. The place of the relevant intermediary rule could be considered, as well as the relevant Hague Convention (Law Applicable to Certain Rights in Respect of Securities held with an Intermediary) on this matter. With regard to protection against losses, regulation could include requirements/provisions for investor insurance, priority rules for investors (in a property law sense) in custodian insolvency, as well as priority rules for a deficit/losses claim against the insolvent estate.

86. In order to offer protection against commingling, asset segregation should be required. Property rights in specific assets could be given to investors. This could be achieved through regulations requiring the creation of specific accounts for custodians and for investors. While this did not necessarily solve the issue of commingling of assets of investors amongst themselves, it would at least allow for segregation between the investors' and the custodian's assets. Operational segregation often resulted in legal segregation, depending upon the applicable law. Segregation, particularly in common law countries, could be achieved through trust. In civil law countries, a statute might be necessary to ensure segregation. Private solutions may also be available, such as the incorporation of specific investor asset vehicles which would safeguard client ownership rights.

'Custody Issues: Developing Practices' – Stephen Keen

87. *Mr Keen* examined the US regime developed for custody of crypto-assets. He noted that a recent study showed that of the 28 companies that provided custody services in digital assets to institutional clients, 14 were domiciled in the US, whereas 3 were domiciled in each of Hong Kong, Switzerland, and the UK. The range of digital assets covered was quite broad, from Bitcoin only to all possible cryptocurrencies. He noted that in the US, there were two main aspects of regulation in this area: the first was regulation of the custodians which provided such services. Various US financial intermediaries required authorisation to act as custodians of assets held through DLT. These were divided into three categories: (i) federally chartered banks and thrifts, (ii) state-chartered banks and trust companies (where the most extensive regulations had been developed), and (iii) federally licensed brokers/dealers. He noted the July 2019 statement issued by the SEC (U.S. Securities and Exchange Commission) and FINRA (Financial Industry Regulatory Authority) identified the issues which brokers/dealers in this area should consider, but without providing any answers.

88. The second aspect related to regulation of users of custody services. For example, federally registered investment advisers were required to use 'qualified custodians', which could be US banks and thrift institutions, US registered broker/dealers, US registered futures commission merchants (FCMs), or a foreign financial institution that customarily held financial assets for its customers. Additionally, federally registered investment companies were required to maintain their assets at US banks and agencies of foreign banks, or members of a US securities exchange (i.e., registered broker/dealers).

89. In the US, some States had 'merit' regulation of digital custody, which limited which assets could be held by custodians based on the regulator's concerns regarding the use of certain cryptocurrencies. Among these, the New York Department of Financial Services ("DFS") imposed the most extensive regulations, which included requiring a licensee to adopt specific policies and procedures for vetting a digital asset before offering custodial services; posting a "greenlist" of virtual currencies approved for custody, which licensees could hold immediately upon giving notice to DFS; requiring that a licensee submit information on other digital assets to the DFS for review before holding such digital assets; and requiring that a licensee may not "facilitate, or knowingly allow the transfer or transmission of virtual currency when such action would obfuscate or conceal the identity of an individual customer or counterparty," (i.e., no "privacy" cryptocurrencies).

90. Mr Keen noted that individuals and institutional custodians faced similar types of issues. This included the use of hot (online) or cold (offline) storage – most custodians used a combination of both. There was also the issue of omnibus or separate wallet model – most custodians also used a combination of these for different types of storage. Although multi-signature wallets were a standard, they presented issues regarding adequate controls over the use of signatures.

91. Other means of protecting against the loss of cryptocurrencies include required capitalisation of the custodian, usually at levels set by State regulators based on expected risks. Insurance was another measure to be considered, with most custodians having insurance ranging from 125-250 million USD, and the coverage possibly being limited to cold storage or other circumstances. Another

step which some custodians took to manage risks was a System and Organisation Controls Reports (SOC 2), which was an audit of the system with a publicly available report.

92. It was noted that US custodians typically complied with the security entitlement provisions (part 5) of the UCC Article 8 to regulate custody of their customers' assets. Article 8 UCC provided a large amount of flexibility which was useful in this area. As such, notwithstanding its title ("Investment Securities"), parties could agree to extend Article 8 to other financial assets (§8-102(a)(9)(iii)); moreover, a security entitlement to a financial asset was created when "a securities intermediary indicated by book entry that a financial asset had been credited to the person's securities account" ((§8-501(b)(1)). Additionally, Part 5 of Article 8 liberally allowed the securities intermediary's duties to be varied by agreement (e.g., (§8-504(c)(1)). Through this, custodians and customers could agree that a digital asset was a financial asset, and that custodians could obtain and maintain digital assets through DLT.

93. Mr Keen noted issues within security entitlements to digital assets. The primary issue was in trading of digital assets. U.S. securities markets provided a gap between a trade (an agreement to buy/sell) and its settlement (delivery of security against payment). This gap allowed the customer's agent (broker/adviser) to trade and then instruct custodians as to settlement. Many cryptocurrency markets did not have such a gap because the user trades by sending the cryptocurrency to a smart contract for immediate settlement. As such, consideration needed to be given as to how a custodian could limit the agent's use of the cryptocurrency. A secondary issue related to encumbrances upon digital assets held in custody. A securities intermediary could not grant a security interest in financial assets held in securities accounts unless agreed by the entitlement holder (§8-504(b). If cryptocurrencies were treated as "general intangibles," they could be easily swept into security agreements. As such, consideration needed to be given as to how a customer could tell if a given cryptocurrency was previously encumbered.

94. Lastly, it was noted that the US Securities and Exchange Commission had recently approved registration statements for two investment companies with transfer agents that would use DLT to issue, redeem and transfer uncertificated shares. Transfer agents for investment companies must be registered with and regulated by the SEC. To this end, the registered transfer agent's version of the distributed ledger was treated as the "official record", whereby those held on other nodes within the DLT were treated as "courtesy copies". However, all versions operated through the same protocol, hence the transfer agent did not have independent access to transaction records or control over blocks. This arrangement treated a decentralised system as though it were centralised via the transfer agent by creating a distinction between "official" vs. "courtesy copy" which allowed the SEC to ignore other users of the protocol. This raised various key issues which needed further exploration.

95. A participant raised a query concerning the notion of custody in general, especially with regard to situations of direct holding, where an owner shared their private key with another party as part of a multi-signature arrangement for security purposes. The question was whether any party who partakes of a multi-signature arrangement which could block transactions in an asset, be treated as a custodian of the asset for private law or regulatory purposes; especially keeping in mind the consequences of a lack of liquidity which were noted in the Lehman Brothers insolvency whereby custody had to be proven in court. It was noted that the rationale behind requirements for custodians were put in place (in the US) to prevent advisors from misusing assets of their customers. In any case, a custodian would largely only act at the direction of the owner of an asset. It was also noted that this consideration was important in situations where multi-signature arrangements existed not for security purposes, but rather as multiple holders of the same asset, and one of the keyholders played a crucial role in transacting the asset. In such situations, putting a regulatory custodial obligation on such a party could be useful.

96. A participant queried what would be the civil law equivalent of a common law trust arrangement to offer protection to the client. It was also queried where there existed a custodian

that held digital assets which did not fall under Article 8 UCC, and if so, how would such a relationship be characterised in US law. It was noted that Bitcoin presented better traceability than other cryptocurrencies, and in the case of a traceable transaction, under civil law (particularly in the Netherlands), a property law interest could be proved in a certain asset. It would be different in an omnibus setting where Bitcoin were spent as a consequence of an algorithm used by a custodian, which was using a Bitcoin pool held by clients. In such a case, a specific property law interest could not be ascertained in a specific asset. This referred to the issue of commingling, which would perhaps require a statutory set of rules to offer protection to clients. Absent proof of ownership, the possessor was assumed to the owner, and the client would be left with only a contractual claim in the asset. It was added that such a situation could be resolved by having a separate (from the custodian assets) pool for the clients' assets on a statutory basis. The clients would be ranked as co-owners, who would share on a *pro-rata* basis in the pool, and not share assets with the custodian. The other solution would be SPVs created and incorporated solely to hold client assets. With regard to the US, it was noted that while bailments were the last resort, they could be a useful mechanism with regard to digital assets. However, bailments were not useful in an omnibus setting or in a setting where there was commingling with the custodian's assets.

97. A participant queried whether the regulatory regime in the State of Wyoming or the State of New York dealt with the insolvency of the custodian. It was noted that they did not specifically deal with the issue. However, it may be possible that SPVs in Wyoming would be subject to receivership under bank regulations, which were applicable. There was an open question as to whether the exclusion of banks from US bankruptcy law extended to trust companies, which could be another issue to consider.

98. A participant queried how the problem of a key being stolen rather than forgotten was to be addressed, especially in a situation where the legitimate holder or the custodian of the key might not even notice that someone else had accessed and used their password. It was noted that using multi-signature wallets prevented such problems. Cybersecurity risks for custodians were another major problem and required further consideration. It was noted that inspiration to resolve these issues could be drawn from how thefts in bank accounts were regulated. In this regard, questions of burden of proof would also need to be considered.

99. A participant queried the importance of future digital assets being designed in a manner more focussed on direct holding in order to provide greater certainty and security, while also allowing for protection of liquidity, perhaps as a result of technology neutral legislation designed to facilitate such thinking. It was noted that the development of Bitcoin was initially spurred largely to reduce the role of intermediaries; however, a commercial need for intermediation had since emerged. It was noted that digital assets more user-friendly to direct holding were already under development.

Session 5 - Conclusion

100. The final session of the Exploratory Workshop on Digital Assets and Private Law included conclusions from the preceding sessions presented by the session chairs, Ms Louise Gullifer, Mr Marek Dubovec, Ms Nina Luisa-Siedler, and Mr Charles Mooney Jr. The session was chaired by Mr Hideki Kanda.

101. The chairs of the sessions thanked all the panellists for their presentations and noted the high quality of content and discussion over the course of the Workshop. It was noted that all the questions and considerations raised would be very valuable in assisting the work to be conducted by the UNIDROIT Working Group on Digital Assets and Private Law.

102. *Mr Kanda* noted two key observations: Firstly, UNIDROIT's role in this area was to provide greater legal certainty to all the parties involved in transactions of digital assets. For this, consistency

of terminology was very important and a functional approach was desirable. Secondly, a distinction between native and non-native digital assets was preferable to a distinction between endogenous and exogenous digital assets. This was because there existed a large amount of legal material on negotiable instruments, investment securities, etc., which could be examined for comparative analysis.

103. He examined the need for legal rules in this area and noted the importance of these in order to offer greater legal certainty, predictability, and confidence to all parties involved in transacting with digital assets. Mr. Kanda thanked all the participants and session chairs for their efforts and involvement in the Exploratory Workshop, as well as the Secretariat for organising the Workshop.

104. The *Secretary-General of UNIDROIT* thanked all the participants and session chairs for their involvement with the Workshop. He thanked Mr. Kanda for leading the work of the Exploratory Working Group which preceded the Workshop and for developing the Workshop's agenda. He noted the importance of work in the area of digital assets and private law and looked forward to the continued collaboration of experts in this area with UNIDROIT. Noting no additional points, he closed the Exploratory Workshop on Digital Assets and Private Law.

ANNEX 1

Exploratory Workshop on Digital Assets and Private Law

17-18 September 2020, 13.00 – 17.00 CEST
Rome and Zoom

Agenda

DAY 1 – Thursday, 17 September

12:30 – 13:00 Registration / Opportunity for online participants to test Zoom connection

13:00 – 13:20 Opening Remarks – *Prof. Ignacio Tirado – UNIDROIT Secretary-General*

13:20 – 14:50 **Session 1 – Digital Assets: A Legal Taxonomy and Challenges to Private Law**

This session will consider some of the more fundamental challenges regarding the application of private law concepts to digital assets, including the application of property law concepts to digital assets, the difficulties in developing a legal taxonomy of digital assets and the challenges in mapping private law concepts onto assets based on a new, and ever-developing, technology.

Chair: *Prof. Louise Gullifer – University of Cambridge*

Panellists: Jason Grant Allen (Humboldt University), Tetsuo Morishita (Sophia University), David Fox (University of Edinburgh)

14:50 – 15:20 Break

15:20 – 16:50 **Session 2 – Legal Issues in the Use of Digital Assets as Collateral: Existing and Emerging International Standards**

This session will discuss various legal issues surrounding the use of digital assets as collateral for loans. It will first provide illustrations of the typical transactions and then examine how the existing and emerging international standards, including the UNCITRAL Model Law on Secured Transactions and the ALI-ELI Principles for a Data Economy address legal issues that arise in secured transactions. The Panel will identify the aspects of secured transactions that the current UNIDROIT project on digital assets should explore in coordination with these standards.

Chair: *Dr. Marek Dubovec – Kozolchyk National Law Center*

Panellists: Andrew Hinkes (Carlton Fields), Steve Weise (Proskauer Rose LLP), Teresa Rodríguez de las Heras Ballell (Universidad Carlos III de Madrid)

DAY 2 – Friday, 18 September

13:00 – 14:20 **Session 3 – Digital Assets Linked to Real-World Assets (Digital Twins): Civil Law and Private International Law Implications**

This session will focus on exploring the issues of digital twins which represent a real-world asset and typically face problems of how to prevent the digital twin from separating from the real-world asset which it represents. The speakers will explain how their respective jurisdictions deal with these issues. In addition, all speakers will share their practical experiences with the multi-jurisdiction issues faced by many, if not all, digital asset projects, realising that in most cases more than one jurisdiction is claiming to be applicable to their digital asset.

Chair: *Dr. Nina-Luisa Siedler – DWF Germany*

Panellists: Thomas Nägele (NÄGELE Attorneys), Joshua Klayman (Linklaters), Urszula McCormack (King & Wood Mallesons)

14:20 – 14:40 Break

14:40 – 16:00 **Session 4 – Intermediated Digital Assets: Custody Issues**

This session will address the settings in which an acquirer of digital assets may choose to hold the assets through a custodian and will compare "direct" holding with various structures for custodial holding. It will explore the practical and legal aspects of custodial holding from the perspectives of an acquirer and a custodian, including issues of private law and insolvency law.

Chair: *Prof. Charles Mooney, Jr. – University of Pennsylvania*

Panellists: Carla L. Reyes (Southern Methodist University), Matthias Haentjens (University of Leiden), Stephen A. Keen, Esq. (Perkins Coie LLP)

16:00 – 16:20 Break

16:20 – 17:00 **Concluding Session**

Chair: *Prof. Hideki Kanda – Gakushuin University – UNIDROIT – Governing Council Member*

Panellists: Chairs of the previous sessions

ANNEX 2

List of Registered Participants

Registered Name	**Affiliation (as provided during registration)**
Adriana Dreyzin	National University of Cordoba
Alan D. Cohn	Steptoe
Alexander Kunzelmann	UNCITRAL
Alisa P. "Paige" Mason	Guidepost Solutions LLC
Álvaro Bourkaib	CUATRECASAS
Analia Gómez Bohle	Profesor
Andrea Tosato	UPENN
Andrew Hinkes	Carlton Fields
Anna Veneziano	UNIDROIT Secretariat
Anselmo María Martínez Cañellas	UIB
Antonio Javier Prado Domínguez	Consultoría Tecnológica e Innovación
Antony W Beaves	Bank of England
Árpád Geréd	MAYBACH • GÖRG • LENNEIS & PARTNER
Arushi Goel	KoineArth
Atsushi KOIDE	Professor, Gakushuin University Faculty of Law
Attila Menyhárd	UNIDROIT Governing Council Member
Bénédicte Fauvarque-Cosson	UNIDROIT Governing Council Member
Bob Trojan	NATLAW
Camilo Isaí Saldías Robles	Universidad de Chile
Carla L. Reyes	Southern Methodist University
Carlo Di Nicola	UNIDROIT Secretariat
Carlos Fernández	Consultoría Tecnológica e Innovación
Carmen Tamara Ungureanu	UNIDROIT Governing Council Member
Casey Scott Laxton	Office of the Comptroller of the Currency
Cemre Kadioglu	UNIDROIT Intern
Charles Kerrigan	CMS Cameron McKenna Nabarro Olswang LLP
Charles Mooney	EWG
Christian TWIGG-FLESNER	University of Warwick
Courtenay R Dunn	ICE Mortgage Services, LLC | MERSCORP Holdings, Inc.
Cristina Frattone	Roma Tre University
Cristina Martínez	
David Fox	EWG
Dror Shapira	INVIOU
Edoardo Ruzzi	Student
Edward John Jones	Student
Edwin E. Smith	Morgan, Lewis & Bockius LLP
Elena Zaccaria	Brunel University
Eugenia Dacoronia	UNIDROIT Governing Council Member
Eva Micheler	LSE
Filippo Zatti	Sapienza Univ. Rome

Francesca Pellegrini	European Banking Institute
Gillian L. Warmflash	J.P. Morgan
Giovanni Rinaldi	
Greg Murphy	Polymath
Hamza Hameed	UNIDROIT
Henry Gabriel	UNIDROIT Governing Council Member
Heribert M. Anzinger	Universität Ulm
Hideki Kanda	GC/EWG
Hugo Dupree	Law Commission of England and Wales
Ignacio Tirado	UNIDROIT Secretariat
Iota Nassr	OECD
Jaime Lopez	Grainchain
Jaime Lopez	GrainChain
Jason Grant Allen	Humboldt-Universität
Jeffrey Ritter	
Jeffrey Wool	EWG
Jess Cheng	The Board of Governors of the Federal Reserve
Jimena Campuzano	REGISTRADOR DE LA PROPIEDAD
John P Burton	Rodey Law
Jose Maria Chozas Plasencia	Ernst & Young Abogados
José Ramón Morales	GARRIGUES
Joshua Klayman	Linklaters
Justice Ricardo Lorenzetti	UNIDROIT Governing Council Member
Katarzyna Królikowska	UNIDROIT Intern
Kathleen Lannan	UNCITRAL
Keisuke Takeshita	Hitotsubashi University
Keith Rowley	
Klaus Löber	Head of Oversight, DG Market Infrastructure and Payments, European Central Bank
Kostoula, Theodora	Sir Roy Goode Scholar at UNIDROIT
Kumiko Koens	Yamagata University
Laura Burgoyne	Law Commission
Louise Gullifer	EWG
Lucas Adomeit	Former UNIDROIT Intern
M. Ece Uyanık	
Manasa Addepalli	Attorney-General's Department Austalia
Marek Dubovec	EWG
María Isabel Carmona	
Maria José Martínez Gómez	Bankia Madrid
Matthias Haentjens	University of Leiden
Megumi Hara	Gakshuin University
Melissa Ford	Attorney-General's Department Austalia
Miriam Bazan	
Monica jalongo	
Monika Pauknerová	UNIDROIT Governing Council Member

Nancy A Rigby	U.S. Bank
Nicholas Filer	Attorney-General's Department Austalia
Nihad Agadazi	Intern UNIDROIT
Niklaus Meier	GC
Nina-Luisa Siedler	EWG
Oscar Suárez	Oxford
Paolo Saguato	George Mason University
Pavel Zold	Czech lawyer
Pedro Méndez de Vigo	CUATRECASAS
Peter Hunn	Clause.io
Peter M Werner	International Swaps & Derivatives Association
Pierre Simonet	IT consultant
Richard Salter	University of Oxford
Ruslan Popov	International law firm in Prague
Sandra M. Rocks	Cleary Gottlieb Steen & Hamilton LLP
Sara Esclapés Membrives	Consultoría Tecnológica e Innovación
Sarah Green	Law Commission
Sarah Worthington	Cambridge
Sessano Altieri	Chuck's Student
Shubha Sastry	Assistant Legal Adviser, Office of the Legal Adviser. U.S. Department of State
Siobhan McKeering	Law Commission
Sonja Maire	Swiss Federal Office of Justice
Sophia Le Vesconte	Linklaters LLP
Souichirou Kozuka	Gakushuin University
Stephen A. Keen	Perkins Coie LLP
Stephen Y. Chow	Hsuanyeh Law Group PC
Steve Weise	Proskauer Rose LLP
Teresa Rodríguez de las Heras Ballell	Universidad Carlos III de Madrid
Tetsuo Morishita	Sophia University
Thibault Langlois-Berthelot	Master 2 student at Paris Nanterre University (2019/2020)
Thomas Keijser	Radboud University
Thomas Mayer	Swiss Federal Office of Justice
Thomas Nägele	
Urszula McCormack	King & Wood Mallesons
Valérie Tweehuysen	Radboud Universiteit Nijmegen
Victoria Garin Gimenez	
Walter K. Oetzell	Walter K. Oetzell APC
Weishi Yang	Law Commission of England and Wales
William Vaudry	Law Commission of England and Wales
Yair Zehavi	INVIOU
Donna Redel	Fordham Law School
Monique Bachner	Bachner Legal