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

EN

Digital Assets and Private Law Working Group
Fourth session (hybrid)
Rome, 2 – 4 November 2021

UNIDROIT 2021
Study LXXXII – W.G.4 – Doc. 2
English only
October 2021

ISSUES PAPER

1. This document provides a discussion of the issues that the Digital Assets and Private Law Working Group may wish to consider in its ongoing work in preparing the prospective guidance document.

2. The issues considered in this document were identified by:

(i) Working Group experts during a series of Exploratory Working Group sessions held between July and September 2020;

(ii) The participants in an Exploratory Workshop on Digital Assets and Private Law held on 17 – 18 September 2020;

(iii) Feedback received from Members of the UNIDROIT Governing Council at its 99th session (23 – 25 September 2020);

(iv) Feedback received from Working Group experts and observers at the First Session (17 – 19 November 2020), the Second Session (16 – 18 March 2021), and the Third Session (31 June – 2 July 2021);

(v) Participants in Sub-Groups as part of intersessional work conducted between January and October 2021;

(vi) The Chair of the Working Group, and

(vii) The Secretariat.

3. The document is divided into two sections: (i) preliminary matters and (ii) scope of the prospective guidance document. Moreover, the document presents the outcome of the intersessional work carried out by the various Sub-Groups and includes a number of preliminary draft principles with commentary and illustrations. It also raises a number of questions that the Working Group may wish to consider.

4. The document contains a number of annexes: **Annex I** contains links to relevant documents to assist the Working Group; **Annex II with Appendices** provides the full list of participants in the Sub-Groups set up to carry out intersessional work; and **Annex III with Appendices** contains the draft Principles with commentary and illustrations, organised thematically by Sub-Group.

TABLE OF CONTENTS

I. PRELIMINARY MATTERS

A. Background

5. In 2015, the Secretariat received a proposal from the Ministry of Justice of Hungary to consider the development of model laws in the domain of "business informatics".[1] In November 2016, the Ministry of Industry and Trade of the Czech Republic sent a proposal to the UNIDROIT Secretariat to include two main topics in the Work Programme: distributed ledger (or blockchain) technology and inheritance of digital properties (see UNIDROIT 2017 – C.D. (96) 5, Appendix II). The Czech Republic submitted a second proposal to UNIDROIT's Governing Council at its 97th session (Rome, 2-4 May 2018), during which the Council concluded that the Secretariat should continue to monitor developments in this area with a view to its possible inclusion in the future Work Programme (see UNIDROIT 2018 – C.D. (97) 19, para. 245).

6. Similarly, the Czech Republic presented a proposal to the UNCITRAL Secretariat requesting that UNCITRAL closely monitor developments relating to legal aspects of smart contracts and artificial intelligence. At its 51st session (New York, 25 June-13 July 2018), the Commission decided that "[t]he Secretariat should compile information on legal issues related to the digital economy, including by organizing, within existing resources and *in cooperation with other organizations*, symposiums, colloquiums and other expert meetings, and to report that information for its consideration at a future session."[2]

7. In line with the joint proposal of the Czech Republic and having received a similar mandate from their governing bodies, UNIDROIT and UNCITRAL agreed to explore the possibility of future joint work in this area. Both organisations agreed that it would be necessary first to identify the most adequate areas of possible work and later to narrow down the scope of the work as well as to define its nature. In light of this, it was decided that two workshops would be held, convening international experts on the different subject matters encompassed by the initial proposal of the Czech Republic.

8. A first joint, invitation-only, workshop was convened at UNIDROIT's seat (Rome, 6-7 May 2019). The workshop gathered leading experts, particularly in the fields of distributed ledger technology (DLT), smart contracts and areas of artificial intelligence.[3] The Governing Council, at its 98th session (Rome, 8-10 May 2019), was informed that the joint workshop had revealed great interest in the area, with particular reference to a general project on digital assets. It was further noted that this project "would require work on categories and conceptualisations, in order to develop a set of definitions for terminologies and concepts used within this area", which in turn "would entail establishing a taxonomy of terms used as part of the digital economy"[4] (see UNIDROIT 2019 – C.D. (98) 17, para. 267).

9. The Governing Council asked the Secretariat to "conduct further research to narrow down the scope of the project", which, based on the conclusions of the joint workshop, "would be initially confined to digital assets", with a decision on final scope to be taken by the Council at its 99th session. The Council also recommended that the Secretariat "conduct additional research on the impact of Smart Contracts/DLT/AI on existing UNIDROIT instruments" (see UNIDROIT 2019 – C.D. (98) 17, para. 275).

[1] UNIDROIT 2016 – C.D. (95) 13 rev., Annex II.

[2] See Report of the United Nations Commission on International Trade Law, UNGA Doc. A/73/17 (51st session, 25 June – 13 July 2018), para. 253, available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/V18/052/21/PDF/V1805221.pdf?OpenElement (emphasis added).

[3] For further information, the Summary of the Discussion and Conclusions from that workshop can be found here: https://www.unidroit.org/english/news/2019/190506-unidroit-uncitral-workshop/conclusions-e.pdf.

[4] The idea for the development of a taxonomy of digital assets and private law concepts was first proposed by Prof. Jeffrey Wool at the 6-7 May 2019 joint UNIDROIT-UNCITRAL workshop event held in Rome.

10. The Governing Council recommended to the General Assembly that it include this Project at medium priority on the 2020-2022 Work Programme (C.D. (98) 17, para. 275). The General Assembly, at its 78th session, approved the inclusion of the project in the Work Programme of the organisation for the 2020-2022 triennium as recommended by the Governing Council (A.G. (78) 12, paras. 43 and 51, and A.G. (78) 3) paras. 69-71). The General Assembly asked the Secretariat to more precisely determine the scope of the project and present it for reconsideration at the next session of the Governing Council.

11. To carry out the mandate received from the General Assembly, a second joint UNIDROIT and UNCITRAL workshop was convened at the UNCITRAL Secretariat in Vienna on 10-11 March 2020. As the previous meeting, this event was an invitation-only meeting of experts, many of whom had also taken part in the first workshop. The invitation was extended with the aim of developing "a legal taxonomy of key emerging technologies and their applications". This second event focused exclusively on the drafting of a taxonomy as well as on the potential relevance of new technologies to existing instruments.

12. On the basis of the discussions during the first and second workshops (Rome, 6-7 May 2019, and Vienna, 10-11 March 2020, respectively) a document was submitted to the Governing Council at its 99th session (A) (C.D. (99) A.4, paras. 23-33) setting out the Secretariat's proposal on the most appropriate scope for this project. Following feedback received from the Governing Council at its 99th session (A), the Secretariat prepared an amended proposed action and the Governing Council agreed to approve the scope and upgrade the level of priority (C.D. (99) A.8, paras. 57-58).

13. Carrying out the mandate received from the Governing Council, the Secretariat set up an Exploratory Working Group, chaired by Professor Hideki Kanda, which held five meetings between July and September 2020 and prepared a preliminary draft of this Issues Paper. Additionally, the Exploratory Working Group facilitated the organisation of an Exploratory Workshop on Digital Assets and Private Law which was held on 17 and 18 September 2020 in a hybrid manner.

14. The Secretariat presented the result of the deliberations of the Exploratory Working Group and the outcomes of the Exploratory Workshop at the September session of the 99th UNIDROIT Governing Council (C.D. (99) B.4 rev.). Following deliberations, it was confirmed to proceed with this project at high priority, allowing the Secretariat to establish a Working Group ("WG") (C.D. (99) B Misc. 2, paras. 7 and 8). The Governing Council approved the temporary change of name of the project to "Digital Assets and Private Law" and provided inputs regarding the structure and composition of the future Working Group, which would also be assisted by a Steering Committee with a broad membership, with experts from different fields (both technical and legal), ensuring an appropriate diversity in terms of geography, legal systems, and gender.

B. Format of the Guidance Document

15. It is anticipated that the Working Group will prepare a set of principles with commentary and illustrations (not – at this stage – a model law or convention) which would include a legal taxonomy relating to digital assets, plus consideration of legal issues arising in particular contexts. A functional approach to legal concepts was deemed to be most appropriate in order to produce a set of Principles which would not be jurisdiction specific, but which could be applied and reflected in any given legal system or culture. The Principles are to embody best practice and international standards and would enable jurisdictions to take a common approach to legal issues arising out of the holding, transfer and use of digital assets across a variety of use cases.

16. For possible templates, the Working Group may wish to consider other existing UNIDROIT instruments such as the UNIDROIT Principles on the Operation of Close-Out Netting Provisions and the UNIDROIT Legislative Guide on Intermediated Securities.

C. Target Audience

17. As consistent with all UNIDROIT instruments, the prospective guidance document should be relevant for both common law and civil law States and would aim to reduce legal uncertainty which practitioners, judges, legislators, and market participants would face in the coming years in dealing with digital assets.

D. Title of the instrument

18. As mentioned above, it is anticipated that the instrument will be in the form of a set of principles and legislative guidance in the area of digital assets and private law. Once the project has advanced sufficiently, the Governing Council's endorsement will be sought for a revised title.

E. Terminology

Use of Standard Definitions

19. One of the objectives of the project is to come up with a legal taxonomy relating to digital assets which is to be developed in coordination with UNCITRAL. Accordingly, it is important that care be taken to ensure accuracy as well as uniformity and consistency across the terms used by both organisations.

Consistency of terminology with existing instruments

20. Existing instruments use different terminology for related concepts. The WG will need to consider which terminology the guidance document should use. Particular attention will be paid to the terminology used in key instruments of reference such as the UNCITRAL Model Law on Electronic Records (e.g., "electronic transferable record" and "control") as well as the UNIDROIT Convention on Substantive Rules for Intermediated Securities (2013) and the UNIDROIT Legislative Guide on Intermediated Securities (2017).

F. Composition of the Working Group

21. Consistent with UNIDROIT's established working methods, the Working Group is composed of experts selected for their expertise in the fields of property law, secured transactions, and digital technology and the law. Experts participate in a personal capacity and represent the world's different systems and geographic regions.

22. The Digital Assets and Private Law Working Group is composed of:

- Hideki Kanda, (Chair), Professor, Gakushuin University (Japan)
- Jason Grant Allen, Senior Research Fellow, Humboldt University of Berlin (Australia)
- Reghard Brits, Professor, University of Pretoria (South Africa)
- Marek Dubovec, Executive Director, Kozolchyk National Law Center (NatLaw) (United States)
- David Fox, Professor, University of Edinburgh (United Kingdom)
- Louise Gullifer, Professor, University of Cambridge (United Kingdom)
- Matthias Haentjens, Professor, Leiden University (Netherlands)
- Hannah Yee-Fen Lim, Associate Professor, Nanyang Technological University, Singapore (Australia)
- Charles Mooney, Jr., Professor, University of Pennsylvania (United States)
- Philipp Paech, Associate Professor, LSE (Germany)

- Carla Reyes, Assistant Professor, Southern Methodist University (United States)
- Nina-Luisa Siedler, Partner at DWF (Germany)
- Luc Thévenoz, Professor, Université de Genève (Switzerland)
- Jeffrey Wool, Senior Research Fellow, Harris Manchester College, University of Oxford (United States)
- Mimi Zou, Fellow, Oxford University (China)

23. UNIDROIT also invited a number of organisations with expertise in the field of digital assets and private law to participate as observers in the Working Group. Participation of these different organisations will ensure that different regional perspectives are considered in the development and adoption of the instrument. It is also anticipated that the cooperating organisations will assist in the regional promotion, dissemination, and implementation of the guidance document once it has been adopted. The following organisations have been invited to participate as observers in the Working Group:

- The World Bank Group
- The United Nations Commission for International Trade Law (UNCITRAL)
- The Hague Conference on Private International Law (HCCH)
- The International Monetary Fund (IMF)
- Association Internationale Des Sciences Juridiques / International Association of Legal Science (AISJ/IALS)
- International Union of Judicial Officers (UIHJ)
- The European Central Bank (ECB)
- The European Banking Authority (EBA)
- The European Banking Institute (EBI)
- Asociación Americana De Derecho Internacional Privado (ASADIP)
- The American Law Institute (ALI)
- The European Law Institute (ELI)
- Kozolchyk National Law Center (NatLaw)
- *Banca d'Italia* (Central Bank of Italy)
- Law Commission of England and Wales
- The Uniform Law Commission (ULC)
- *Istituto per la vigilanza sulle assicurazioni* (The Institute for the Supervision of Insurance) (IVASS)
- The Italian Financial Services Authority (CONSOB)

24. Finally, UNIDROIT may also invite a number of industry associations to participate as observers in the Working Group to ensure that the guidance document will address the private sector's needs. The latter will also assist in promoting the implementation and use of the guidance document. The following private sector association has been invited to participate as an observer in the Working Group, but more may be invited:

- The International Swaps and Derivatives Association (ISDA)

G. Methodology and Organisation

25. Under the guidance of its Chair Professor Hideki Kanda, the Working Group will undertake its work in an open, inclusive, and collaborative manner. As consistent with UNIDROIT practice, the

Working Group will not adopt any formal rules of procedure and seek to make decisions through consensus.

26. The preparation of a guidance document on Digital Assets and Private Law is a high priority project on the UNIDROIT Work Programme (2020-2022). The following would be a tentative calendar, the effective execution of which may be affected by the evolution of the current extraordinary international context:

(a) Drafting of the guidance document over five sessions of the Working Group in 2020-2022:

- First session: 17-18-19 November 2020 (remote)
- Second session: 16-17-18 March 2021 (remote)
- Third session: 30 June – 1-2 July 2021 (hybrid)
- Fourth session: 2-3-4 November2021 (hybrid)
- Fifth session: 7-8-9 March 2022 (hybrid)
- It is envisaged that, in between in-person sessions, remote meetings may be conducted when deemed necessary. Given the extraordinary circumstances, one or more of the in-person meetings may be substituted by remote webinars.

(b) Consultations and finalisation: 2022 – 2023

(c) Adoption by the Governing Council of the complete draft at its 102nd session in May 2023.

H. Establishment of a Steering Committee

27. In light of the very broad interest generated by this new project and its inherently global and interdisciplinary nature, at its 99th session the Governing Council decided in favour of an "enhanced" structure for the project which would entail the setting up of a Steering Committee on Digital Assets and Private Law in addition to the establishment of a Working Group (C.D. (99) B Misc. 2, paras. 7 and 8). It is envisaged that the Steering Committee will be comprised of experts from different fields (both technical and legal) and is expected to act in a consultative capacity, to allow for wider participation, ensuring all sensitivities and domestic realities are considered, increase transparency, and provide invaluable context-specific feedback to the Working Group.

28. The Steering Committee is chaired by Professor Monika Pauknerová, member of the UNIDROIT Governing Council. So far, thirty-six experts have been nominated to the Steering Committee by twenty-five Member States, plus the European Commission.

II. SCOPE OF THE GUIDANCE DOCUMENT

A. Relationship with existing instruments and other projects of the current Work Programme

29. This section briefly introduces how this project would benefit from existing instruments and feed into – and hence create synergies – with other projects of the current Work Programme.

30. In terms of the relationship with existing UNIDROIT instruments, important aspects envisaged in the Digital Assets and Private Law project concern the legal analysis of transfers and the taking of security over digital assets, issues relating to the provision of digital asset custody services, and issues relating to the insolvency of the custodian of digital assets. These items naturally link with the Institute's work in capital markets and, more precisely, in the area of intermediated securities,

providing connections with existing instruments such as the UNIDROIT Convention on Substantive Rules for Intermediated Securities (2013) and the UNIDROIT Legislative Guide on Intermediated Securities (2017).

31. Regarding synergies with other projects of the current Work Programme, there is a natural fit with the Best Practices of Effective Enforcement project, which will undertake the analysis of the impact of new technologies on enforcement as one of its main objectives. This constitutes a natural opportunity for cross-fertilisation between the two projects, and, to this end, a number of experts involved in the Exploratory Working Group on the Digital Assets project have already been contacted to help identify concrete examples of the application of new technologies in the context of enforcement. Additionally, a workshop organised on 21 September 2020 on Enforcement featured a panel on the impact of new technologies on enforcement with presentations delivered on a taxonomy of technological applications in enforcement proceedings, smart contracts and enforcement, and enforcement and digital assets.

32. Another area which presents an opportunity for cross-cutting work is the joint UNIDROIT – UNCITRAL project concerning a Model Law on Warehouse Receipts. There is a direct relationship with this project which examines the issuance and transfer of electronic warehouse receipts for goods stored in warehouses. In this connection, one of the categories of digital assets to be examined in the Digital Assets project concerns digital tokens which are linked to an external non-digital asset. By fostering exchanges between the two Working Groups, the legal analysis undertaken in the context of both projects would be mutually enriched. Moreover, should the work in the project to draft a Model Law on Factoring cover receivables issued in the form of digital assets, the cross-fertilisation between both projects would also bring about important benefits.

33. Additionally, this project also has synergies with a project on Best Practices in the Field of Electronic Registry Design and Operation which is run by the Cape Town Convention Academic project, in partnership with the UNIDROIT Foundation, Aviareto, and the Aviation Working Group. This project is developing a best practice guide for electronic registries, focused on collateral registries, which may be an important element of a system of digital assets, particularly when used as collateral.

B. General: Private law relating to Digital Assets, in particular proprietary interests

34. The Working Group is invited to focus on private law issues relating to digital assets and in particular proprietary interests with a view to assessing the extent to which rules provided under typical common law and civil law systems are appropriate—or not—for digital assets. It is envisaged that the project will offer solutions not only where gaps exist, but where the traditional approaches would not be appropriate and should be modified. Where necessary, the discussion will seek to (i) explain various technological aspects, (ii) identify the issues that may arise in the absence of specific laws and regulations, and (iii) suggest Principles that the private law regime should incorporate.

35. In terms of the most appropriate approach, the WG agreed that the project should seek to articulate the practical problems involving digital assets as well as the desired outcomes which should be the same across all legal systems. The principles would state the desired outcome, and then leave it to each State to determine how their legal system would achieve the desired outcome rather than dealing with the legal nature of digital assets in each and every legal system, an approach that represented the highest level of functionality and had the advantage of not requiring that States modify their property law or insolvency law. It was further noted that a problem-solving approach would not preclude the project from providing further guidance on how the desired outcomes could be achieved in practice, and that, where considered to be appropriate and feasible, the commentary accompanying the principles could provide further guidance which States could consider regarding how to reach the desired outcome. For example, secured transactions could be a good candidate for an area where further guidance could be provided as there was an existing package for States wishing

to carry out reforms to consider. Overall, the consensus was that the right approach was the one which provided the needed clarity and legal certainty, without necessarily prescribing a given path for harmonisation.

36. The project will primarily address private law issues which could nevertheless present certain regulatory aspects. While regulation *per se* is outside the scope of this project, given that there are a number of aspects touched upon by the project which border on regulatory issues, the Working Group may wish to take these into account to ensure coherence between the recommendations for private law and any regulatory approaches. The connection is more pronounced in some aspects of this project, such as custody given that a large number of the assets under discussion are held by custodians and intermediaries.

C. The subject matter of the project

37. As part of the intersessional work that the Working Group agreed upon at its first session, Sub-Group 4 was set up with a dual focus on taxonomy as well as questions relating to private international law. **Co-Chairs Philipp Paech and Elisabeth Noble** led the participants in **Sub-Group 4** as they examined a range of issues relating to taxonomy of digital assets from a private law perspective. (A full list of the participants is available at **Annex II, Appendix 4**).

38. At the Working Group's third session, a proposal was made to define a digital asset as follows: "A digital asset is an electronic record which is capable of being subject to control." It is noted that this working definition may be subject to further refinement as the Project progresses. Sub-Group 4 also elaborated on a proposed sub-categorisation of digital assets for the purposes of taxonomy. Regarding co-ordination with UNCITRAL, the possibility of carrying out work on a taxonomy beyond the one done for the purposes of the Principles was noted. The Working Group is invited to consider and discuss the revised paper describing the scope of the taxonomy work stream which was prepared by the co-chairs of Sub-Group 4 (available at **Annex III, Appendix 4**).

The legal nature of a proprietary connection between digital data and another asset

39. Some types of digital data might be created to represent other assets, in such a way that the holder of digital data purports to have a proprietary right to that underlying asset.[5] The digital data in such a structure can be seen as a digital asset in its own right or merely as a digital record. For the purposes of this discussion the former characterisation is assumed. When a digital asset is transferred from A to B, the relevant proprietary right to the underlying asset is also supposed to be transferred. The mechanism of linking one asset to another is sometimes called tokenisation but focusing on 'tokens' may be misleading in a proper legal analysis, since what actually matters is the mechanism itself and the nature of the relevant link.

40. The link between digital and the relevant underlying assets might be viewed in two different ways, although the Working Group may identify other possible options. The first assumes that the digital data is itself a digital asset, and a legal analysis analogous to that of a documentary intangible would apply.[6] The second approach is to view the digital data as constituting the root, or, alternatively, evidence, of title to the underlying asset (as an entry on a register). A question arises whether a special legislation is necessary to recognise digital data as the root of title (as was the case in the U.S. State of Delaware).

[5] This discussion assumes the accuracy of all relevant assumptions and that all "real world" necessary steps have been taken extraneous to the relevant digital asset and platform on which it exists so as to ensure the intended results. For example, it assumes that the relevant "other asset" exists and is at all times maintained in a legally enforceable manner for the exclusive benefit of the holders of the digital assets.

[6] A documentary intangible such as a negotiable instrument is a tangible object (a piece of paper) linked to an intangible so that transfer of that piece of paper transfers the intangible asset.

41. Experts have identified the following list of links between the digital and the underlying assets:

- direct ownership – digital data directly denoting a legal entitlement to the gold;
- equitable ownership – digital data constituting equitable entitlement (under a trust) to the underlying assets:
    - ✓ the "issuer" of digital assets holds the legal title to the underlying assets; and
    - ✓ a third party is the legal owner of the underlying assets;
- ownership in an SPV (Special purpose vehicle) – digital assets constitute interest in an SPV that invests in the underlying assets;
- contractual (personal) right – digital assets evidencing a contractual right towards the "issuer" in relation to the financial returns from the underlying assets.

42. An argument might be made that a law governing proprietary interests in digital assets might then *ipso facto* determine interests in the underlying assets, which would result in legal rules on proprietary interests in every type of underlying assets (not to mention the relevant choice-of-law rules) being affected by that digital assets law. Such a far-reaching law/argument would though be implausible and impractical and the Working Group should agree upon the need for a thorough consideration of the property rights aspects involved in the link between digital data and the relevant underlying asset.

43. As to the categories of "digital twins", at the moment, the following broad types have been identified for the purposes of further discussion:

- Non-fungible tokens (NFTs) - digital assets associated with external art or other object by a technical pointer and/or by a licensing agreement;
- Digital Asset backed by Real-World Assets;
- Digital Assets backed by Digital Assets;
- Decentralised Finance (DeFi).

Illustrations

Non-fungible Tokens (NFTs) – NBA Top Shot

44. NBA Top Shot[7] uses a closed-system platform called Flow, where every member becomes a party to a user agreement and assume the relevant rights and obligations. NBA Top Shot issues an NFT that "contains," a video "moments" from NBA games. Users purchasing "packs" of these moments (the "Art") are granted "a worldwide, non-exclusive, non-transferable, royalty-free license to use, copy, and display the Art … solely...for their own personal, non-commercial use" and then they can sell, swap, or simply display their collection of "moments" online on these conditions, so that the Art never leaves the system.

Question for the Working Group: Should the Principles address or otherwise consider the issues stemming from the possible decoupling of an NFT and the underlying asset when the NFT operates in an open environment (i.e., as opposed to a closed one)?

Digital Assets backed by Real-World Assets – PAX Gold

45. PAX Gold (PAXG) is "a tokenized version of gold that represents real, physical gold", which takes a form of Ethereum-based tokens, with all transactions being subject to an Ethereum blockchain smart contract. The holders of PAXG beneficially own the underlying physical gold held in

[7] Applicable law is the Province of British Columbia and the federal laws of Canada (TOS 17.vi).

custody by Paxos Trust Company in Brink's vaults in London (UK) and, according to the PAXG White Paper suggests, could convert them into physically allocated gold, unallocated gold entitlements or fiat currency.

46. According to the PAXFG's website, "when a customer trades for allocated gold bars, they receive ownership rights to specific gold bars that are held in a precious metal dealer's vault on the customer's behalf" and "when a customer trades for unallocated gold, they do not have actual ownership over specific gold bars; instead, they have a general entitlement to a certain quantity of gold that an institution promises to deliver. This is hypothetical gold and is a liability of the institution that one has a claim against. This is similar to the way a traditional bank operates – customers don't own specific notes, but rather they have a credit that can be paid out upon request. The token holder, hold all of the economic value of the gold represented by your tokens, and all of the risk and reward related to ownership of that gold."

Digital Assets backed by Digital Assets

47. Wrapped Bitcoin[8] is an example of a digital asset backed by a digital asset. The idea is for an asset in one blockchain system to represent the value of another asset in a different blockchain system. A user transfers Bitcoin to a consortium of service providers that then hold the Bitcoin on reserve, and gets a new instrument called "wrapped Bitcoin", which is technically compatible with another blockchain system (e.g., the Ethereum). As a result, the user can then use the value of a Bitcoin as if it were technically compatible with the Ethereum system. It is not clear, however, whether the user could claim his Bitcoin back and on what conditions.

Question for the Working Group: What are the implications for service providers in control of the wrapped assets and does this implicate some kind of custody relationship?

Decentralised Finance (DeFi)[9]

48. DeFi refers to Decentralized Finance, which reflects a decentralized way to execute traditional financial transactions. DeFi operates by virtue of code, it is based on blockchain and open technology, and thus, it is open and available to everyone, without relying on centralized financial intermediaries such as brokerages, exchanges, or banks. DeFi involves transactions with various digital assets, including cryptocurrencies, stablecoins and tokens. These transactions are often structured like collateralized transactions. In those transactions, a DeFi user either borrows funds by granting security over a digital asset or loans out the digital asset in return for a financial compensation. Maker DAO provide one of the most popular DeFi services.

D. Identify specific areas/issues of private law to be addressed

49. A wide range of issues in contract law with respect to digital assets could be identified. Currently, many of these are under thorough examination in various projects by several organisations.[10] Certain legal remedies in connection with the holding, transfer and collateralisation of digital assets may be attributed to contract law.

1. Acquisition, disposition, and competing claims

50. Under the leadership of **Co-Chairs Chuck Mooney, Jr. and Matthias Haentjens**, **Sub-Group 2** examines a range of issues relating to control and transfer of digital assets and has met seven times between January and September 2021 (a full list of the participants is available at **Annex**

[8] Neither WBTC nor RenBTC have user agreements or terms of service. There are potential issues involving code deference (Code deference must be further explained).

[9] DeFi concept is further addressed separately below in the section on SG3.

[10] For a representative and comprehensive study, see the ALI/ELI Principles for a Data Economy at https://www.ali.org/projects/show/data-economy/.

2, Appendix 2). The outcome of these meetings was the preparation of a series of draft principles together with commentary and illustrations (Principle X.1A: Scope of the Principles; Principle X.1B: Definition of 'electronic record'; Principle X.1C: Definition of 'digital asset'; Principle X.1D: Definition of 'control'; and Principle (X.2) on Acquisition and Disposition ('Transfer') of digital assets) (found below for the consideration of the Working Group at **Annex 3, Appendix 2**).

51. Regarding draft Principle (X.2) ("Transfer"), at its second session, the Working Group agreed to further consider: (i) the question of whether innocent acquisition rules ought to be recognised in the context of digital assets, as applied in different jurisdictions; and (ii) the types of digital assets to be covered by the Principles. The Working Group also reached a consensus to the effect that the States should adopt (or retain) a shelter principle in support of the innocent acquisition rule if the Principles adopt such a harmonized innocent acquisition rule. At its third session, further refinements were made to the draft Principle X.2, and the Working Group noted that the commentary might provide more explicit guidance on how different jurisdictions might implement innocent acquisition rules to reflect the best use of existing law and legal theories together with the relevant technological realities.

2. Definition of Control

52. Regarding draft Principle (X.1) "Control", at its second session, the Working Group clarified that the definition of "control" was a factual instead of a legal definition. At its third session, a revised draft Principle on control was presented and it was emphasised that it referred to a general concept of control that was meant to function in the context of transfer (with implications for other aspects of the DAPL project such as custody and secured transactions). The Working Group agreed that further intersessional work was required on the issue of custodial transfer and the implications for control and the innocent acquisition rule, and that the inclusion of a degree of exclusivity was important to narrow down the assets with which the Project was concerned (e.g., to exclude photos and social media posts). The Working Group also agreed on the need to maintain a functional approach and an exclusivity rule with degrees of relaxation.

3. Provision of digital asset custody services

53. Led by **Co-Chairs Louise Gullifer and Luc Thévenoz**, **Sub-Group 1** examines a range of issues relating to control and custody of digital assets and has met seven times between January and October 2021 (a full list of the participants is available at **Annex 2, Appendix 1**). The outcome is draft Principle C on custody which addresses situations where a person (usually a legal person, often a regulated entity) holds a digital asset on behalf of and for the benefit of another, typically a client, in a manner that gives the client special protection against unauthorised dispositions of the asset and against the insolvency of the custodian.

54. At its third session, the Working Group also discussed the definitional boundaries of custodianship in relation to insolvency and minimal custodial duties. It was explained that the notion of custody was one in which the custodian owed some duties to the client in relation to safeguarding assets, and that Sub-Group 1 had endeavoured to set out the custodial duties in the draft custody Principle. The latest version of draft Principle C on custody may be found below at **Annex 3, Appendix 1** for the consideration of the Working Group.

4. Taking of security over digital assets

55. As part of the intersessional work that the Working Group agreed upon at its first session, Sub-Group 3 was set up to examine questions relating to secured transactions in the area of digital assets (a full list of the participants is available at **Annex 2, Appendix 3**). Led by Chair Marek Dubovec, Sub-Group 3 examines a range of issues relating to secured transactions and digital assets and has met six times between January and October 2021. The outcome of these meetings was the

preparation of a series of draft principles together with commentary and illustrations (found below the for the consideration of the Working Group at **Annex 3, Appendix 3**).

56. It is noted that the secured transactions draft Principles are agnostic as to the structure and nature of the secured transactions regime. It is envisaged that they should be implementable in States with a single comprehensive secured transactions law that covers all types of rights in movable assets that secure an obligation, similarly to the UNCITRAL Model Law, as well as in States that approach security rights differently. It is noted that the draft Principles do not take a position about the ideal structure and nature of the secured transactions regime but highlight some aspects of the regimes that may be more conducive to secured transactions involving digital assets, or amenable to amendments.

57. At the third session, Sub-Group 3 presented research which explored how existing paper documents representing possession and title for the purposes of executing secured transactions would be useful analogies to digital assets tethered to real-world assets. It also presented an exploration of DeFi (decentralised financed) and an expert observer presented the structure of liquidity pool tokens. These special sections may be found at **Annex 3, Appendix 3, Sub-Appendix A**).

5. The legal treatment of digital assets in relation to insolvency proceedings

58. Private-law property rules provide an incomplete picture of the legal treatment of digital assets unless the treatment of those rights in insolvency proceedings also are considered. Categorisation of digital assets as some form of property or other rights enables their return to the holder or realisation by the insolvency administrator for the benefit of the estate. Further, realisation of value is not only affected by legal categorisation, but also the factual nature of digital assets.

59. Given that the private law treatment of digital assets as property may affect whether digital assets belong to a debtor's insolvency estate[11], the Working Group may wish to consider the treatment of digital assets in the insolvency proceedings of various parties such as the "owner" of digital assets (assuming that the Working Group arrives at the conclusion that they are amenable to ownership in the legal sense), as well as custodians and intermediaries which would include the exchange service providers (e.g. crypto-fiat exchange service providers, crypto-exchange service providers, crypto-asset stock exchange), or others holding security interests in the concerned assets.

60. As insolvency laws do not generally provide for rules specific to the treatment of digital assets, the Working Group may deem it desirable to conduct assessment of those approaches as to their suitability to digital assets and possible adaptations. A further nuance is that digital assets may be treated differently depending on their respective nature. Insolvency laws apply different rules to proceeds in the form of cash and its equivalents, which some digital assets, especially cryptocurrencies may be categorised as. Consequently, the Working Group may wish to consider exploring the need for and the methods of ensuring that the rights of the holders of digital assets would have the same treatment in insolvency proceedings as the rights in intellectual property and other intangibles.

61. The Working Group may also wish to consider other issues relating to insolvency proceedings, such as the valuation of digital assets (sharp fluctuations in value from the time of the filing to distribution may significantly impact the recovery of holders or creditors), or the practical challenges of identifying and tracing digital assets in the context of any form of stay of assets and suspension of actions in insolvency proceedings.

[11] See UNCITRAL Legislative Guide on Insolvency Law, Recommendation 35

6. Remedies and Enforcement

62. The project will also have to consider issues of proprietary remedies and enforcement. In the first instance, this will require some engagement with the remedial mechanisms available in different legal systems and their appropriateness to intangible objects of proprietary rights (i.e., digital assets). In the civil law context, for example, questions will arise as to whether the remedy of *vindication* is available (especially in jurisdictions where the status of digital assets as "things" is unclear). Civil law systems typically distinguish between possessory and petitory remedies, such that the answer to questions such as whether digital assets are capable of possession, and whether "control" is analogous to possession, will determine the scope of remedies available. Across the common law world, there are divergent approaches to the question whether rights in intangibles can be protected by means of the tort of conversion. Issues are also likely to arise in the context of trusts. An important subset of questions under this section relates to following and tracing digital assets through transaction pathways that may be novel, as they are based on new technologies and business models.

63. In all cases, a general issue arises as to how property rights can be enforced over digital assets given the nature of the technical system in which digital assets are created, held, and dealt with. For example, where a distributed ledger system does not rely on a central counterparty with the authorisation to change the ledger in response to a court order, questions will arise concerning how property rights are enforced on the relevant ledger. However, the general question of how to enforce property rights in case of unknown possessors is not new *per se*, and it may be that existing concepts can be adapted to deal with enforcement of property rights to digital assets.

64. The project may also have to consider other issues relating to enforcement in addition to those discussed above. Issues relating to the enforcement of judgments over digital assets represent a point of articulation between the study and the UNIDROIT Study LXXVI on Principles of effective enforcement. The project may also benefit from the emerging work at UNCITRAL on civil assets tracing and recovery.[12] Decentralized, anonymous, autonomous, and irrevocable processes involved in distributed ledger technology (DLT) have raised unique challenges for the tracing and recovery of certain digital assets (e.g., cryptocurrency), particularly in insolvency for the purpose of enforcing the rights of creditors. An UNCITRAL Colloquium discussed various challenges that arise from tracing and recovering digital assets such as cryptocurrencies, air miles, and virtual online game items.

65. At its first session, the Working Group noted the importance of considering enforcement as part of the Project while acknowledging the presence of another UNIDROIT project in this area (Enforcement Project). The Secretariat will ensure that there is coordination on this point between the two projects as work continues to progress. The WG further noted the importance for the project to arrive at principles which envisaged private law remedies that would apply as broadly as appropriate to digital assets which used different kinds of technical systems; some of which were more or less amenable to conventional enforcement. It is therefore expected that questions relating to remedies and enforcement will be addressed at the appropriate junctures in the various workstreams being carried out in the context of intersessional work.

7. Law applicable to issues relating to digital assets

66. Developing Principles for the law applicable to digital assets presents another set of challenges. Issues may relate to the determination of the applicable law, jurisdiction, and the question of the choice of forum. The scope of this Project is limited to the issues of applicable law, while other issues are likely to be explored by the Hague Conference on Private International Law or

[12] See UNCITRAL, Report of the Colloquium on Civil Asset Tracing and Recovery (Vienna, 6 December 2019), para. 25 (UNCITRAL, Feb. 2020).

other organisations[13] On this note, the WG agreed at its first session that close collaboration and coordination with the HCCH regarding PIL matters (applicable law) was highly desirable.

67. At its second session, the Working Group agreed on three issues to be addressed by the tentative Principles (available at **Annex III, Appendix 4**): (i) the law applicable inside the digital assets platform (network)[14] and, in particular, the law covering acquisitions and dispositions (the same law should apply to transfers and collateralisation on a given network); (ii) conflict of laws in relation to "digital twins"; and (iii) conflict of laws in relation to insolvency-related issues. On the latter, the Working Group noted that, for the purposes pf certainty, the law applicable to a transaction in question should be given preference over the law of insolvency proceedings, however, this might come into conflict with other principles of different legal systems. The Working Group agreed to consider a hybrid approach.

[13] In particular, the HCCH is looking at the possibility of a new normative project in this area which would look at applicable law, jurisdiction, recognition and enforcement, choice of law, and choice of forum. The Permanent Bureau of the HCCH has published a preliminary document regarding "Developments with respect to PIL implication of the digital economy, including DLT" (Prel. Doc. No 4 of November 2020), and the HCCH's Council on General Affairs and Policy recently confirmed the mandate for the PB to continue to follow private international law implications relating to developments in the field of DLT. See HCCH, *Conclusions & Decisions*, Council on General Affairs and Policy, 1-5 March 2021.

[14] Regarding choice of terms between "platform" and "network", the WG agreed that "network" was preferable.

ANNEX I

ADDITIONAL RESOURCES

Unidroit Instruments

Unidroit, Convention on International Factoring (1988).

Unidroit, Convention on International Interests in Mobile Equipment (2001).

Unidroit, Convention on Substantive Rules for Intermediated Securities (2013).

Unidroit, Legislative Guide on Intermediated Securities (2017).

Unidroit, MAC Protocol (2019).

Unidroit, Principles of International Commercial Contracts (2016).

Unidroit, Principles on the Operation of Close-Out Netting Provisions (2013).

UNCITRAL Instruments

UNCITRAL, Model Law on Electronic Transferable Records (2017).

UNCITRAL, Model Law on Secured Transactions (2016).

UNCITRAL, United Nations Convention on the Assignment of Receivables in International Trade (New York, 2001).

HCCH Instruments

HCCH, Convention of on the Law Applicable to Certain Rights in Respect of Securities held with an Intermediary, (Hague Securities Convention, 5 July 2006).

Other Organizations

American Law Institute & European Law Institute, "ALI–ELI Principles for a Data Economy - Data Rights and Transactions", Draft No. 2 (2018).
Abstract: A report compiling and collating existing and potential legal rules applicable to transactions in data as an asset and as a tradeable item that also assesses the 'fit' of those rules to these transactions.

European Commission, *Investment services and regulated markets - Markets in financial instruments directive (MiFID)*, accessed June 2021.
Abstract: A repository of documents and studies related to the markets in financial instruments directive (Directive 2004/39/EC). In force from 31 January 2007 to 2 January 2018, the directive governed provision of investment services in financial instruments by banks and investment firms and operation of traditional stock exchanges and alternative trading venues, while also addressing the interplay between these systems and emerging technologies.

European Commission, "REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-assets", Legislative Proposal, Document 52020PC0593, amending European Union Directive 2019/1937 (24 Sept. 2020).

ABSTRACT: a proposal to enable and support the potential of digital finance including: a pilot regime on distributed ledger technology (DLT) market infrastructures, digital operational resilience, and changes to certain related European Union financial services rules.

Financial Stability Board (FSB) "Decentralised financial technologies: Report on financial stability, regulatory and governance implications" (6 June 2019).
ABSTRACT: This report considers several forms of decentralisation in financial services and identifies technologies that are decentralising – or may in the future decentralise – financial activities. It makes a preliminary assessment of which financial services are beginning to, and may in the future, incorporate such technologies.

G7 Working Group on Stablecoins, "Investigating the Impact of Global Stablecoins" (2019).
ABSTRACT: A report investigating the legal challenges for domestic and cross-border implementation of a stablecoin digital currency, looking at private and regulatory law implications for private providers as well as considerations for public entities such as central banks and regulatory authorities.

G30 Working Group on Digital Currencies, "Digital Currencies and Stablecoins – Risks, Opportunities, and Challenges Ahead" (2020).
ABSTRACT: This report examines the landscape of digital currencies and highlights issues that policymakers must consider, including the balance that must be struck between the protection of individual data versus the government's imperative to enforce laws, regulations, and taxes, addressing issues for central banks and financial regulators.

Global Blockchain Business Council (GBBC), "Global Standards Mapping Initiative (GSMI) Report (2020)" (October 2020).
ABSTRACT: Provides technical standards and legislative guidance released by sovereign and international bodies regarding blockchain based on a broad survey of jurisdictions and industry consortia.

International Monetary Fund (IMF), "Fintech: The Experience So Far" (2020).
ABSTRACT: The paper finds that while there are important regional and national differences, countries are broadly embracing the opportunities of fintech to boost economic growth and inclusion, while balancing risks to stability and integrity.

International Monetary Fund (IMF), "Fintech Notes – The Rise of Digital Money" (2019).
ABSTRACT: This paper identifies the benefits and risks and highlights regulatory issues that are likely to emerge with a broader adoption of stablecoins. The paper also highlights the risks associated with e-money: potential creation of new monopolies; threats to weaker currencies; concerns about consumer protection and financial stability; and the risk of fostering illegal activities, among others.

International Organization of Securities Commissions (IOSCO), "Global Stablecoin Initiatives" (2020).
ABSTRACT: This paper includes some background to the genesis and development of the paper, together with an overview of different stablecoin designs, a hypothetical case study, application of current IOSCO Principles and Standards to global stablecoin, and an assessment of the broader implications for securities regulators.

International Organization of Securities Commissions (IOSCO), "Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms" (Feb. 2020).
ABSTRACT: This report describes issues and risks identified to date that are associated with the trading of crypto-assets on CTPs. In relation to the issues and risks identified, it describes key considerations and provides related toolkits that are useful for each key consideration. These key considerations and toolkits are intended to assist regulatory authorities who may be evaluating CTPs within the context of their regulatory frameworks.

International Swaps and Derivatives Association (ISDA), "Private International Law Aspects of Smart Derivatives Contracts Utilizing Distributed Ledger Technology" (Jan. 2020).

ABSTRACT: This paper considers the private international law, or conflict-of-law, aspects of derivatives contracts governed by the laws of Singapore and England and Wales involving distributed ledger technology (DLT), commonly known as blockchain technology. This paper will identify specific private international law issues with respect to contract law that may arise when trading derivatives in a DLT environment and, where appropriate, will propose recommendations on how these issues might be clarified or resolved.

Organisation for Economic Co-operation and Development (OECD), "The Tokenisation of Assets and Potential Implications for Financial Markets" (2020).

ABSTRACT: This report analyses the impact that wide-spread adoption of tokenisation could have, discusses emerging opportunities and risks of the application of DLTs for financial markets and their participants, illustrated with case studies in OECD and non-OECD economies. It investigates the role of trusted third-party authorities in decentralised networks as guarantors of the connection between the on- and off-chain worlds, and explores the need for a tokenised form of central bank currency or stablecoin for the payment leg of security settlements on DLT-based trading venues.

Perkins Coie LLP, CoinLaw, available for download for Apple iPhone IOS and Google Android as of June 2021.

ABSTRACT: The Perkins Coie CoinLaw app provides an international update and high-level summary of each nation's current stance on virtual currencies.

Stanford Law School CodeX, *RegTrax Regulatory Database*, The Stanford Centre for Legal Informatics, accessed June 2021.

ABSTRACT: An open-source platform and a resource for global blockchain regulations, including discussion forums and conversations among practitioners and experts.

World Bank Group (WBG), "Distributed Ledger Technology & Secured Transactions: Legal, Regulatory and Technological Perspectives – Guidance Notes Series Note 1: Collateral Registry, Secured Transactions Law and Practice" (May 2020).

ABSTRACT: This Guidance Note examines the potential of Distributed Ledger Technology (DLT) within the context of the UNCITRAL Model Law on Secured Transactions. While this model is the primary reference, the Guidance Note also provides examples from domestic secured transactions frameworks, especially where the analysis leads to a different result. It examines these issues from different perspectives, including those of policy makers and legislators but also secured creditors and borrowers.

World Bank Group (WBG), "Distributed Ledger Technology & Secured Transactions: Legal, Regulatory and Technological Perspectives – Guidance Notes Series Note 2: Regulatory Implications of Integrating Digital Assets and Distributed Ledgers in Credit Ecosystems" (May 2020).

ABSTRACT: This guidance note focuses on the regulatory implications that the deployment of distributed ledger technology (DLT) entails for secured transactions and collateral registry (STCR) frameworks. It examines the regulatory regimes applicable to three DLT-STCR outputs: the use of digital assets implementing DLT as collateral, the application of DLT in platforms supporting secondary markets for the valuation and disposal of collateral, and the application of DLT in collateral registries.

World Bank Group (WBG), "Distributed Ledger Technology & Secured Transactions: Legal, Regulatory and Technological Perspectives – Guidance Notes Series Note 3: Distributed Ledger Technology and Secured Transactions Frameworks: A Primer" (May 2020).

ABSTRACT: This Guidance Paper provides a primer on distributed ledger technology (DLT) and highlights the junctures at which this new technology meaningfully impacts secured transactions frameworks. The aim is to identify legal and regulatory hotspots, laying the groundwork for their detailed and exhaustive analysis, which is carried out in the two companion papers, Notes 1 and 2.

United Nations Internet Governance Forum (IGF), *Dynamic Coalition on Blockchain Technologies (DC-Blockchain)*, accessed June 2021.

ABSTRACT: A repository of discussion and substantive work papers exploring actual and potential applications of and issues relating to blockchain technology, as well as blockchains larger policy implications for larger topics such as cybersecurity, data rights and privacy, and the growth of the Internet of Things (IoT).

ANNEX II

INTERSESSIONAL WORK

(January to October 2021)

Full list of participants in the Sub-Groups

Appendix 1 – SUB-GROUP 1 – Control and Custody

Co-chairs Louise Gullifer and Luc Thévenoz led the participants in Sub-Group 1 as they examined a range of issues relating to control and custody of digital assets. A full list of the participants is available below. The Sub-Group held virtual meetings on the following dates:

SG1 – First Meeting – 19 January 2021 14:00-15:30 (CET)

SG1 – Second Meeting – 05 February 2021 14:00-15:30 (CET)

SG1 – Third Meeting – 23 February 2021 14:00-15:30 (CET)

SG1 – Fourth Meeting – 13 April 2021 14:00-15:30 (CEST)

SG1 – Fifth Meeting – 29 April 2021 14:00-15:30 (CEST)

SG1 – Sixth Meeting – 2 June 2021 14:00-15:30 (CEST)

SG1 – Seventh Meeting – 5 October 2021 14:00-16:00 (CEST)

List of Participants

Ms Louise GULLIFER *Co-Chair*	Rouse Ball Professor of English Law University of Cambridge United Kingdom
Mr Luc THEVENOZ *Co-Chair*	Professor Université de Genève Switzerland
Mr Jason Grant ALLEN	Senior Research Fellow Humboldt University of Berlin Australia
Mr David FOX	Professor of Common Law School of Law University of Edinburgh United Kingdom
Mr Matthias HAENTJENS	Professor of Law Leiden University the Netherlands
Mr Hideki KANDA	Professor of Law Gakushuin University Japan

Ms Hannah Yee-Fen LIM	Associate Professor Nanyang Technological University *Singapore*
Ms Carla REYES	Assistant Professor of Law SMU Dedman School of Law Dallas, United States of America
Ms Nina-Luisa SIEDLER	Partner DWF Germany
Ms ZOU Mimi	Fellow University of Oxford China
Mr Jeremy BACHARACH (*Observer*)	Visiting Researcher Harvard Law School United States of America
Mr LIU Hin (*Observer*)	Oxford DPhil student and tutor at Oxford and Hong Kong University Fusang
EUROPEAN BANKING INSTITUTE (EBI) (*Observer*)	Mr Matthias LEHMANN Professor Universität Wien EBI Germany
Mr Klaus LÖBER (*Observer*)	Germany

Appendix 2 – SUB-GROUP 2 – Control and Transfer

Co-chairs Matthias Haentjens and Charles Mooney, Jr., led the participants in Sub-Group 2 (SG2) as they examined a range of issues relating to control and transfer of digital assets. A full list of the participants is available below. The Sub-Group held virtual meetings on the following dates:

SG2 – First Meeting – 20 January 2021 15:00-17:00 (CET)

SG2 – Second Meeting – 10 February 2021 15:00-17:00 (CET)

SG2 – Third Meeting – 24 February 2021 15:00-17:00 (CET)

SG2 – Fourth Meeting – 11 May 2021 15:00-17:00 (CEST)

SG2 – Fifth Meeting – 25 May 2021 15:00-17:00 (CEST)

SG2 – Sixth Meeting – 9 September 2021 15:00-17:00 (CEST)

SG2 – Seventh Meeting – 30 September 2021 15:00-17:00 (CEST)

List of Participants

Mr Matthias HAENTJENS *(Co-Chair)*	Professor of Law Leiden University the Netherlands
Mr Charles MOONEY Jr. *(Co-Chair)*	Professor of Law University of Pennsylvania United States of America
Mr Jason Grant ALLEN	Senior Research Fellow Humboldt University of Berlin Australia
Mr Marek DUBOVEC	Executive Director Kozolchyk National Law Center (NatLaw) United States of America
Ms Hannah Yee-Fen LIM	Associate Professor Nanyang Technological University Singapore
Ms Carla REYES	Assistant Professor of Law SMU Dedman School of Law Dallas, United States of America
Ms Nina-Luisa SIEDLER	Partner DWF Germany
Mr Andrew (Drew) HINKES *(Observer)*	Attorney at Law K&L Gates United States of America

AMERICAN LAW INSTITUTE (ALI) *(Observer)*	Mr Steven WEISE Partner United States of America
KOZOLCHYK NATIONAL LAW CENTER (NatLaw) (*Observer*)	Mr Bob TROJAN Senior Advisor United States of America
LAW COMMISSION OF ENGLAND AND WALES *(Observer)*	Ms Miriam GOLDBY Professor of Shipping, Insurance and Commercial Law Queen Mary Univ London United Kingdom
	Ms Sarah GREEN Professor Commissioner for Commercial & Common Law
EUROPEAN BANKING INSTITUTE (EBI) *(Observer)*	Mr Matthias LEHMANN Professor Universität Wien EBI

Appendix 3 – SUB-GROUP 3 – Secured transactions

Chair Marek Dubovec led the participants in Sub-Group 3 as they examined a range of issues relating to secured transactions in digital assets. A full list of the participants is available below. The Sub-Group held virtual meetings on the following dates:

SG3 – First Meeting - 21 January 2021 14:30-16:00 (CET)

SG3 – Second Meeting – 18 February 2021 13:45-15:15 (CET)

SG3 – Third Meeting – 20 April 2021 15:00-16:30 (CET)

SG3 – Fourth Meeting – 18 May 2021 15:00-16:30 (CEST)

SG3 – Fifth Meeting – 11 June 2021 15:00-16:30 (CEST)

SG3 – Sixth Meeting – 13 October 2021 15:00-16:30 (CEST)

List of Participants

Mr Marek DUBOVEC *(Chair)*	Executive Director Kozolchyk National Law Center (NatLaw) United States of America
Mr Reghard BRITS	Associate Professor University of Pretoria South Africa
EUROPEAN CENTRAL BANK (ECB) (*Observer*)	Mr Klaus LÖBER Head of Oversight DG Market Infrastructure and Payments Germany
HAGUE CONFERENCE ON PRIVATE INTERNATIONAL LAW (HCCH) (*Observer*)	Ms Gérardine GOH ESCOLAR First Secretary Permanent Bureau the Netherlands
KOZOLCHYK NATIONAL LAW CENTER (NatLaw) (*Observer*)	Mr Bob TROJAN Senior Advisor United States of America
UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAW (UNCITRAL) (*Observer*)	Mr Jae Sung LEE Legal Officer International Trade Law Division Austria
AMERICAN LAW INSTITUTE (ALI) (*Observer*)	Mr Steven WEISE Partner United States of America
Mr Andrew (Drew) HINKES (*Observer*)	Attorney at Law K&L Gates United States of America

EUROPEAN BANKING INSTITUTE (EBI) (*Observer*)	Mr Matthias LEHMANN Professor Universität Wien EBI Germany
Ms Theodora KOSTOULAS (*Observer*)	PhD Candidate European University Institute Italy
Mr Gavin MCCOSKER (*Observer*)	Australia

Appendix 4 – SUB-GROUP 4 – Taxonomy & PIL

Co-Chairs Philipp Paech and Elisabeth Noble led the participants in Sub-Group 4 as they examined a range of issues relating to the creation of a taxonomy of digital assets for private law purposes, as well as issues relating to private international law. A full list of the participants is available below. SG4 held virtual meetings on the following dates:

SG4 – First Meeting – 26 January 2021 16:00-17:30 (CET)

SG4 – Second Meeting – 16 February 2021 14:00-15:30 (CET)

SG4 – Third Meeting – 2 March 2021 14:00-15:30 (CET)

SG4 – Online consultations – 23 September–7 October 2021

List of Participants

Mr Philipp PAECH *(Co-Chair)*	Associate Professor London School of Economics & Political Science Germany
EUROPEAN BANKING AUTHORITY (EBA) *(Observer) (Co-Chair)*	Ms Elisabeth NOBLE Senior Policy Expert Banking Markets, Innovation and Products United Kingdom
Mr Matthias HAENTJENS	Professor of Law Leiden University the Netherlands
Mr Hideki KANDA	Professor of Law Gakushuin University Japan
Ms Louise GULLIFER	Rouse Ball Professor of English Law University of Cambridge United Kingdom
Ms Carla REYES	Assistant Professor of Law SMU Dedman School of Law Dallas, United States of America
Mr Luc THEVENOZ	Professor Université de Genève Switzerland
Mr Jeffrey WOOL	Senior Research Fellow Harris Manchester College, University of Oxford United States of America
HAGUE CONFERENCE ON PRIVATE INTERNATIONAL LAW (HCCH) *(Observer)*	Ms Gérardine GOH ESCOLAR First Secretary Permanent Bureau the Netherlands

KOZOLCHYK NATIONAL LAW CENTER (NatLaw) (*Observer*)	Mr Bob TROJAN Senior Advisor United States of America
UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAW (UNCITRAL) *(Observer)*	Mr Alexander KUNZELMANN Legal Officer International Trade Law Division Austria
Monika PAUKNEROVÁ GCm	Prof. JUDr. Monika Pauknerová, CSc. DSc. Department of Business Law Charles University Faculty of Law Czech Republic
AMERICAN LAW INSTITUTE (ALI) *(Observer)*	Mr Steven WEISE Partner United States of America
THE INTERNATIONAL SWAPS AND DERIVATIVES ASSOCIATION (ISDA) *(Observer)*	Mr Peter WERNER Senior Counsel United Kingdom
INTERNATIONAL MONETARY FUND (IMF) *(Observer)*	Ms Marianne BECHARA Senior Counsel Legal Department United States of America
EUROPEAN BANKING INSTITUTE (EBI) *(Observer)*	Mr Matthias LEHMANN Professor Universität Wien EBI Germany
UNIFORM LAW COMMISSION (ULC) (*Observer*)	Mr Andrea TOSATO Associate Professor of Commercial Law University of Nottingham (United Kingdom) Visiting Associate Professor in Law University of Pennsylvania (USA)
Mr Klaus LÖBER (*Observer*)	Germany
Mr Jeremy BACHARACH (*Observer*)	Visiting Researcher Harvard Law School United States of America
Mr LIU Hin (*Observer*)	Oxford DPhil student and tutor at Oxford and Hong Kong University Fusang

ANNEX III

DRAFT PRINCIPLES AND COMMENTARY

Appendix 1 – SUB-GROUP 1 – Control and Custody

PRINCIPLE C – Custody

C.1 This Principle applies when, in the course of a business and pursuant to an agreement, a person (called a custodian) holds a digital asset on behalf of a client in a manner that the asset so held is not available to the creditors of the custodian if the custodian enters into insolvency proceedings. The agreement between the custodian and the client is called a custody agreement.

This Principle applies to custody, that is, to situations where a person (usually a legal person, often a regulated entity), holds a digital asset on behalf of and for the benefit of another, typically a client, in a manner that gives the client special protection against unauthorised dispositions of the asset and against the insolvency of the custodian. It only applies when the person providing the custody services does so in the course of a business.

It is quite common that the same business carries out various activities other than custody, including maintaining fiat accounts for its clients, trading digital assets on its clients' accounts, trading digital assets on its own account, operating a marketplace ("exchange" or "trading platform"), etc. This Principle only applies to the service of custody, irrespective of other activities carried out by the person providing this service and irrespective of the business' regulatory status. Whenever the word 'custodian' is used, it refers to that person insofar as it is providing custody services. Whatever this principle states about custodians only applies to custody services and not to other services provided by those persons.

The purpose of this Principle is to set out principles relevant to custody of digital assets. This first paragraph is a general statement explaining the core situation in which there is a custody agreement and in which a person acting in the course of a business is a custodian. It is designed to be helpful to the reader and is not drafted as a legal definition. There will be situations when there is a custody agreement where the custodian does not hold a digital asset on behalf of a client: (1) if the client has not yet transferred a digital asset to the custodian or the custodian has not yet received it on behalf of the client; (2) when the custodian has exercised a (limited) right of use (see C.4(i)); or (3) if a custodian breaches its obligations and fails to hold the digital asset that is the subject of the custody agreement. Moreover, it is difficult to see how a person (in the course of a business) could hold an asset on behalf of a client in a way that it is available to the 'custodian's' creditors since if this is the case the 'custodian' would have complete ability to use the asset as its own and the asset would not be held on behalf of the client. The general statement, however, captures the two critical points of custody, namely, that in most situations the 'custodian' holds the asset (and the client does not) and yet the asset does not form part of the custodian's insolvency estate. 'Hold' is defined in C.2. The commentary at the end of this principle explains the different ways in which a digital asset can be held.

C.2 In this principle –

(a) when a digital asset is considered fungible, a reference to the asset must be construed as a reference to a certain quantity of assets of an identical type to that digital asset;

(b) a person (including a custodian) holds a digital asset if –

(i) that person controls the asset, or

(ii) a custodian provides custody services to that person in relation to the asset.

The purpose of C.2(a) is to enable the principle to apply to fungible digital assets without this situation having to be mentioned explicitly in every paragraph.

The purpose of C.2(b) is to introduce the concept of 'holding' a digital asset, which is wider than the (factual) concept of 'control' as defined in the Control Principle. The word 'hold' is defined as encompassing two situations. The first is where a person, either a custodian or another person such as an investor, controls an asset within the meaning of the Control Principle. The second is where a person is the recipient of custody services, that is, where a custodian controls the asset on behalf of that person. If the recipient of the custody services is itself a custodian, the person who controls the asset is a 'sub-custodian'. Where a sub-custodian is used, the sub-custodian, the custodian and the client all 'hold' the asset. If the recipient of the custody services is not a custodian, the person who controls the asset is a custodian, and the custodian and the client 'hold' the asset.

C.3 An agreement for services to a client in relation to a digital asset is a custody agreement if

(a) the service is provided in the course of the service provider's business,

(b) the service provider is obliged to obtain (if this is not yet the case) and to hold the asset on behalf of the client, and

(c) the client does not have control of the digital asset;

unless it is clear from the wording of the agreement that the client does not have the protection described in C.9.

C.3 provides a method to identify whether an agreement is a custody agreement or not. It does two things. First, (a), (b) and (c) serve as a definition of a custody agreement, and therefore of custody. Second, it addresses the line between a custody agreement and an agreement under which any assets held by the service provider form part of that service provider's assets for distribution to its creditors on its insolvency. This latter type of agreement can look similar to a custody agreement, in situations where the client does not have control of the digital asset, and the service provider maintains an account in which the client's entitlement is recorded (which is also (or should be) the case under a custody agreement). However, if under such an agreement any assets controlled by the account provider form part of its assets for distribution to its creditors,, the client is exposed to the insolvency risk of the account provider.. A client taking on such a risk should be aware that it is doing so. , whereas this is not the case under a custody agreement. For this reason, an agreement under which the client does not have control is presumed to be a custody agreement unless it is made clear in the agreement that assets held by the service provider form part of that party's assets available for distribution to its creditors. Principle C.3 is designed act as an incentive to service providers to make the nature of the agreement clear on its face.

A state may wish to protect a client who enters into an agreement which exposes the client to the insolvency risk of the service provider by regulation. Various options for such regulatory protection are set out in [ ].

C.4 A custodian owes the following duties to its client:

(a) the custodian is not authorised to [dispose of] [transfer] that asset, or use it for its own benefit, except to the extent permitted by the client and the law;

(b) the custodian is obliged to [dispose of] [transfer] that asset on the client's instructions; and

(c) the custodian owes duties to the client in relation to the safe-keeping of that asset or of a pool of assets which includes it.

The language of Principle C.4 is intended to be functional and neutral between legal cultures. In some jurisdictions, the custodian/client relationship will be legally characterised as a trust while it may be characterised as a contractual relationship in other jurisdictions.

Principle C.4 sets out duties which are owed by a person providing custody services under an agreement with a client. These are basic duties and a State should not permit them to be excluded by the terms of the intermediary agreement.

(i) This duty refers to the inability of the custodian to use the asset for its own benefit except as permitted by the client and by law. The client may consent to that use either by contract or by an instruction to the custodian, and may consent to a use more limited than that permitted by law.

(ii) This duty makes the basic point that a custodian is a person who must deal with the assets according to the client's instructions.

(iii) This merely states that a custodian owes some duties in relation to safekeeping. A state can choose which safekeeping duties cannot be excluded. Some suggestions are contained in C.6.

C.5 Unless disallowed by a provision in the custody agreement [or by law], a custodian may hold fungible digital assets of several clients in an undivided pool.

Principle C.5 addresses the common situation where a service provider, such as an exchange, holds an undivided pool of assets on behalf of its clients. In a pooled account, the custodian controls a number of fungible digital assets but no assets or private keys are specifically identified on chain as relating to a particular client (see C.6). Instead, the number of assets the custodian holds for each client is recorded in the books of the custodian. There could be many reasons for this situation, but one possibility is that an exchange executes transfers of digital assets between its clients by book entry rather than by changing the control of the digital assets.

C.6 The duties owed by a custodian to its client may include:

(a) the duty to maintain a record of the digital assets it holds for each client;

(b) the duty at all times to securely and effectively hold digital assets in accordance with the records it maintains for its clients;

(c) the duty to acquire digital assets promptly if this is necessary to satisfy the duty under (b);

(d) the duty to keep digital assets held for the account of clients separate from assets held for its own account;

(e) subject to any right granted to the custodian or to another person, the duty to pass all the benefits issuing from a digital asset to the client for whom it holds that asset.

Principle C.6 sets out duties that a state may include in its list of non-excludable duties.

(a) A custodian must maintain a record of the digital assets it holds for every client. That record may either be maintained separately of the distributed ledgers which record the respective digital assets or, if technology allows, be part of the information stored in the distributed ledger.

(b) The custodian owes a duty to hold assets correlating to those records. Thus, if the record shows that a custodian holds 1 BTC for A, the custodian must control at least 1 BTC.

(c) This duty is to replace any missing assets, in other words, to reconcile the custodian's holding to the client records. The assets acquired must, of course, be of an identical type and quantity to the assets recorded in the records.

(d) This duty relates to the basic custodial duty to separate client assets from house assets (ie the custodian's own assets). It does not address the segregation of assets of any particular client. It is assumed that a custodian may either offer a client a fully segregated account or a pooled account (also known as an omnibus account), where the custodian holds assets for a number of clients. *[NOTE: omnibus holdings were present in the MountGox and Cryptopia cases].* A segregated account would be where a custodian controls a number of assets (and the relevant private keys) for that particular client. Any transfer to another client would then have to take place by a change of control. If the digital assets are non-fungible, they can only be held in a segregated account.

(e) The duty to pass on to the client all the benefits of the digital asset is subject to any right granted to the custodian or to another person. The benefits of a digital asset may include voting rights.

C.7 The relationship between the custodian and the client may exist notwithstanding that a third person has rights against the client in relation to the digital asset.

Principle C.4 makes it clear that the client could (in the relevant jurisdiction) hold the asset on trust for someone else (eg the client could be an investment fund or an individual holding the asset for family member) or that the functional equivalent could occur in other jurisdictions.

C.8 A digital asset held by a custodian for a client

(a) may be subject to a security right granted to that custodian by the client;

(b) may be subject to a security right in favour of that custodian arising by operation of law.

Principle C.8 permits a custodian to have a security interest in the asset it controls for a client. The client may owe the custodian fees, for which the custodian wishes to be secured, or the custodian may have lent the client money to acquire the assets. [*Taking security over digital assets is addressed in the Secured Transactions Principles prepared by SG3 where the secured creditor's interest is called a 'security right'. SG3 probably says something about the security right being automatically perfected in this situation (that is the US position) although this is inconsistent with the Financial Collateral Directive in the EU and the relevant regulations in the UK as currently interpreted.*]

C.9 If a custodian enters insolvency proceedings, a digital asset that it holds for the account of a client does not form part of that custodian's assets for distribution to its creditors.

C.9 sets out the consequences of the insolvency of the custodian in a functional way rather than using legal concepts such as property or ownership. On the custodian's insolvency, assets it controls for clients as custodian are not part of the distributed estate. If a holder is not a custodian, any assets it controls will be part of its assets for distribution to its creditors. The effect of C.3 is that any agreement which has the three characteristics of a custody agreement set out in C.3 will attract the consequences in C.9 unless the agreement makes it clear that this is not the case.

C.10 When authorised by a client or by law, a custodian may hold a digital asset for that client through another custodian (a sub-custodian) if the sub-custodian is bound by the duties stated in principles C.4 [and C.6].

C.11 When a custodian holds a digital asset for a client through another custodian:

(a) If the sub-custodian enters insolvency proceedings, the custodian must seek to obtain control of the digital asset from the administrator of the insolvency;

(b) If the custodian enters insolvency proceedings, the rights it has against the sub-custodian in respect of the digital assets held as custodian for its clients do not form part of the custodian's assets for distribution to its creditors.

Examples of custody

[description of 'pure' custody]

[description of an exchange]

[description of custody of a 'tethered' asset]

Examples of situation which are not custody

Where a person, such as an investor, controls a digital asset. A person (such as an investor) can control a digital asset by using some hardware, software, or an online service. This is the case when, for example, she runs a full node (or a light node) on the blockchain on which the asset is registered or when she uses a wallet software or service to access the blockchain. In all these cases, the investor keeps control of the digital asset because she stores and uses the private key and does not entrust or surrender it to a third party. The provider of the wallet used by the investor only provides the means (hardware, software, or service) by which the investor stores and uses her private keys. The investor is exposed to the risk of the wallet malfunctioning, but her digital assets are not controlled by the provider. The insolvency of the provider would affect its ability to operate or maintain the wallet but has no legal impact on the digital assets controlled by the investor. The relationship between the investor and the person providing the service is purely contractual and is governed by the terms of the contact between them.

Safeguarding of private keys. Another arrangement is where a business safeguards its client's private keys or provides software or hardware to facilitate the client's safekeeping its private keys. Depending on the features of this service, the business may (or may not) have the ability to use the client's private keys and thus take control of the client's digital assets. However, this is not the purpose of the service and typically the business will be prohibited from using the client's private keys for any purpose that has not been agreed by the client. The client still has control of the digital asset, and has the ability to change the control of the asset (using the terminology in Principle [Control] (1)(a)(i)). This service is therefore not a custody service as defined in this principle, even though it is sometimes called "custody" by market participants. In contrast, where a business provides a custody service, its clients transfer their digital assets to addresses or private keys controlled by that business, or the business acquires digital assets which it controls on behalf of the client.

Agreement for a deposit account. A Fintech firm or a financial institution, such as a dealer, an exchange or a trading platform may incur an obligation to deliver a certain quantity of a given digital asset to a client because it has received the asset from the client or because it has acquired the asset on the primary or secondary market on behalf of the client. The firm or institution will maintain an account on which credits and debits of a particular digital asset are recorded from time to time so that the account balance evidences at any time the quantity of such digital asset the firm or institution is obliged to deliver to the client (or, as the case may be, may claim from the client). For each digital asset, such an account operates in the same way as a current account in a fiat currency. The investor does not have control of digital assets; she merely has an unsecured personal claim against the account provider. If the account provider becomes bankrupt, the claim for delivery of a digital asset is likely to be converted into a (fiat) money claim and will rank *pari passu* with the claims of all other unsecured creditors. [Please note that if the digital asset is not fungible, the relevant claim is for delivery of a specific asset rather than for a generic quantity of a particular digital asset. This, however, should not alter the legal characterisation of the obligation as a personal right or its treatment as an unsecured claim in the bankruptcy of the obligee.]

A State may consider whether regulation is required to provide protection to some or all types of clients. One option would be to require providers of this type of account to hold a certain amount of capital. This could either be required to be in the form of a particular type of asset (such as the asset which is the subject of the account, or fiat currency) or could be required to be of a particular credit standard, such under the Basel Regulations. This requirement could be accompanied by a preference in relation to such capital for the clients on the insolvency of the account provider. Another option would be to mandate specific disclosure of the relevant risks in the agreement. Another option would be to require providers of this type of account to be regulated entities conforming to particular standards. Yet another option would be to limit the type of people who could become clients to certain types of people (as in many crowd-funding regulations. These options are only suggestions, and could be combined if desired.

Digital autonomous organisation (DAO) use code (also called smart contracts or apps) stored and executed on the blockchain to control certain digital assets. An investor may transfer a digital asset to a particular smart contract so that its code will determine when and to whom the digital asset will be ultimately transferred. This situation is different from direct holding, custody and personal claim if there is no identifiable person, natural or legal, who controls the digital assets subject to the smart contract. In some jurisdictions a DAO can be a legal person, or the smart contracts are controlled by natural or legal persons in which case there is an identifiable person. However, in other cases the DAO is just a web of smart contracts with no involvement of a natural or legal person. The operation of the smart contract may depend on some form of vote or consensus among participants in the blockchain, but a voting or consensus mechanism can hardly qualify as joint control of the assets by all persons entitled to participate in the decision.

Appendix 2 – SUB-GROUP 2 – Control and Transfer

PRINCIPLE [X.1A]
Scope of the Principles

These Principles deal with the private law relating to [transactions in] digital assets.

Explanation and commentary

[To come.]

* * *

PRINCIPLE [X.1B]
Definition of 'electronic record'

'Electronic record' means information which is (i) stored in an electronic or other intangible medium and (ii) capable of being retrieved.

Explanation and commentary

1. A 'digital asset' is a subset of 'electronic record'. Under this Principle, an 'electronic record' consists of information if the information is stored in an electronic or other intangible medium and is capable of being retrieved. It is implicit in the requirement that the information be retrievable that the information also must be retrievable in a form that can be perceived. It follows that an electronic record would not include, for example, oral communications that are not stored or preserved or information that is retained only through human memory.

2. This definition is consistent with the definition of the term 'electronic record' in Article 2 of the UNCITRAL Model Law on Transferable Records and similar definitions in various national laws. See, eg, Uniform Electronic Transactions Act (United States), Article 2(7) (defining 'electronic record'), 2(13) (defining 'record') Were it not for this provenance of the definition it might seem quite odd that the term 'electronic *record*' is defined as 'information' and not as a '*record*' of information (except as might be implicit in the requirement that the information be stored and retrievable). If one were writing on a clean slate, perhaps it would make sense to use the "record of information" formulation. However, the role of this term is solely as a component of the definition of 'digital asset'. As explained in the commentary to the definition of 'digital asset', the determinative factor is whether an 'electronic record' 'is capable of being subject to control'. It follows that either formulation of the definition of 'electronic record' would produce the same result. Given that, it is appropriate and prudent to adopt the approach to the definition of the term that already has been generally accepted.

PRINCIPLE [X.1C]
Definition of 'digital asset'

'Digital asset' means an electronic record which is capable of being subject to control.

Explanation and commentary

1. The definition of 'digital asset' includes an electronic record only if it is 'capable of being subject to control'—as 'control' is defined in Principle [X.1D]. For example, some electronic records may be described colloquially as 'digital assets' but normally could not be subjected to 'control', as defined, and consequently would not be digital assets as defined here.

2. Consider a simplified example: Two sets of information compose an electronic record. One set is 'No Left Turn Unstoned' (NLTU) *plus* information (key information) that, pursuant to public-key cryptography, renders this set of information capable of being subject to control by means of the associated private key. (Note that this does not mean that the key information necessarily

contains the private key itself, but only the information that makes it controllable with the private key.) Those two components—NLTU plus the key information—compose the digital asset (the 'NLTU digital asset'). The second set of information is 'I Gave Her the Ring, She Gave Me the Finger' (IGHTR,SGMTF). Although information consisting of IGHTR,SGMTF is associated with and included in the same electronic record as the NLTU digital asset, a transfer of control of the NLTU digital asset so that it becomes subject to control through different key information would not transfer control of the IGHTR,SGMTF information. Indeed, the IGHTR,SGMTF information is not (it is assumed) capable of being subject to control. This example is not unrealistic. For example, an interest in Bitcoin is composed of an unspent transaction output (UTXO). The UTXO might be associated with information, such as information included in a header, that is a part of the same electronic record as the UTXO but which is not capable of being subject to control. The header information would not necessarily be transferred as a result of spending the UTXO.[15]

3. Continuing with the example of the NLTU digital asset described in comment 2, pursuant to Principle X.2 an innocent acquirer (IA) of the NLTU digital asset would acquire it free of conflicting proprietary claims. But this would not mean that the IA acquires the information NLTU (e.g., that the IA 'owns' NLTU). Instead, the IA acquires the information NLTU only insofar as it is associated with the key information as a part of the NLTU digital asset. The information NLTU itself presumably exists not only as a component of the NLTU digital asset but also independently and separate and apart from the NLTU digital asset. The information NLTU is the same—'No Left Turn Unstoned' is 'No Left Turn Unstoned'—however or wherever that information might be stored, existing, or perceived. The NLTU digital asset is distinct, however, because it is composed not only of the information NLTU *but also of the key information*.

4. The information NLTU might be an image, poem, book, video, song, database, a combination of 1s and 0s without any inherent value, or any other type of information. But whatever its content or characteristics, under these Principles the information would remain subject to any applicable laws other than law governing digital assets contemplated by these Principles (digital assets law). If the information were subject to valid copyright protection, for example, the rights of the holder of the copyright would not necessarily be affected by the creation, acquisition, or transfer of the digital asset. Consistent with this analysis, under [Transfer] Principle [X.2](11) a digital assets law adopting these Principles should be made subject to any conflicting provisions of any applicable intellectual property laws (among other laws that a State might specify). See Illustration [2]. *infra*. On the other hand, it is possible that inclusion of information in a digital asset, or the use, transfer, or acquisition of the digital asset, could violate or infringe upon rights under such laws. Even if the information NTLU (or any other information included in a digital asset) were not subject to any protection under intellectual property or other laws, the existence, use, or rights (if any) in respect of that information outside of and other than as a part of a digital asset would not be affected by a digital assets law.

5. The Illustrations to Principles [X.1.A] (scope of the Principles), [X.1.B] (definition of 'electronic record'), and [X.1C] (definition of 'digital asset'), *infra*, provide additional examples of the application of the definition of digital asset and the scope of these Principles.

6. Given the broad colloquial meaning given to the term 'digital asset', the Working Group may wish to consider whether another term, perhaps one that is more functionally oriented or more closely associated with the concept of control, should be employed to confine the scope of these Principles. Consideration might be given, for example, to 'transferable digital asset' (cf. 'electronic transferable record', defined in Article 2 of the UNCITRAL Model Law) or 'controllable digital asset'.

Illustrations of the application of Principles X.1A (scope of the Principles), X.1B (definition of 'electronic record'), and X.1C (definition of 'digital asset')

Illustration 1: Digital asset is a virtual (crypto) currency on a public blockchain, e.g., Bitcoin.

[15] Examples and discussion in these Principles that draw on blockchain technology or distributed ledger technology generally are not intended to modify or undermine the applicability of these Principles to digital assets that employ other technologies or to impair the technology neutrality of these Principles. This is a general point that is not limited to the discussion here of the definition of 'digital asset'.

In a public blockchain no one person controls the underlying protocol (software)—ie, the blockchain that tracks transactions in the digital assets. A consensus mechanism embedded in the protocol verifies the validity of transactions that users attempt to effect through the protocol. No one individual user has control over the protocol or its consensus mechanism. The underlying protocol (system) for the public blockchain would not be capable of being subject to "control' as defined in Principle X.1.D.). However, an individual user does have control over private keys, which allow the individual user to obtain 'control' (as so defined) over a digital asset within the protocol (ie, over a UTXO (unspent transaction output) in the case of Bitcoin).

Although other public blockchains may differ from Bitcoin as to the applicable consensus mechanism and the manner that transactions are tracked, the foregoing description would apply nonetheless. An individual user could not, alone, control the underlying protocol (the database or blockchain), but could control the user's private key and thereby have 'control' (as defined) over the digital assets held through the protocol. The protocols within which digital assets exist are not themselves digital assets within the scope of these Principles. The assets controlled by private keys however are digital assets within the scope.

The analysis and discussion in Illustration 1 also informs the following Illustrations.

Illustration 2: Digital asset contains information that is a valuable dataset/database (eg, dataset that is the basis for the operation of an AI system), image, or textual expression*.*

If the information included in the digital asset is itself subject to protection under intellectual property law (presumably copyright law, in this example), the rights of the holder of the intellectual property would be preserved notwithstanding the inclusion of the information in the electronic record or the transfer of the digital asset to an innocent acquirer. To the extent permitted by the applicable intellectual property law the transferee of the digital asset might be entitled to the use and enjoyment of the information (not unlike the lawful purchaser of a book protected by copyright). Alternatively, if the information or its functionality were protected by patent law, for example, then the acquirer of the digital asset could be infringing the patentee's rights by using the information.

Although the particular facts of this illustration may not be realistic or reflect common practice, it is intended to illustrate and underscore the point that a digital asset law should be subject to any applicable intellectual property laws. It also illustrates the broader point that a digital asset comprises only the package of information that includes the information necessary to make it capable of being subject to control. The same information that is included in a digital asset and that exists outside of and separate and apart from the digital asset is not a part of the digital asset.

Illustration 3: Digital asset is 'tethered' to another asset.

This Illustration contemplates that pursuant to law other than a digital asset law and any applicable contractual arrangements an acquirer of a digital asset will, *ipso facto*, acquire another asset. That other asset might be entirely exogenous (eg, a physical commodity such as a precious metal) or one that is inherently connected to the digital asset (eg, a security that by its terms may be acquired and disposed of only in connection with the acquisition and disposition of a digital asset within the relevant protocol/platform.

The digital asset is composed only of information capable of being subject to control and the other asset (even if it is itself composed of information) is not a component of the digital asset and is not within the scope of these Principles. For example, under a law conforming to Principle [X.2], an innocent acquirer of the digital asset may take the digital asset free of competing proprietary claims. But other law (and the relevant facts, including the applicable contractual arrangements) would determine whether (and the extent to which) or not the acquirer would take free of (or subject to) competing proprietary claims to the other asset.

Illustration 4: Facebook page with password for access.

Generalizations about social media/social networking platforms are difficult. But Facebook and many other social media platforms generally involve licensing arrangements with users that do not permit the users to acquire 'ownership' of 'pages' or the data stored on the platform. This is so even though colloquially users may refer to 'their' pages and information that 'belongs' to them. In general, these platforms do not allow users to acquire the exclusive abilities contemplated by the

Principle [X.1.D] definition of 'control'. Consequently they do not constitute or involve digital assets within the scope of these Principles.

Illustration 5: Excel or Word file with password protection.

A Word, Excel or similar data file is an electronic record as defined in Principle [X.1.B]. If access to viewing the contents of the file is password protected, then it is possible that one who has knowledge of the password would have the exclusive abilities necessary to obtain control under Principle [X.1.D]. Because the file would be capable of being subject to control, the file would be a digital asset as defined in Principle [X.1.C] and within the scope of these Principles. That said, unless the digital asset were associated with a protocol that facilitates the acquisition and disposition of such assets, laws adopting these Principles would not have any material utility or impact for these assets. One might view this circumstance as indicating that the scope of the Principles is overbroad. However, it is better characterized as merely an example of digital assets that would not normally be disposed of and consequently would not benefit from or involve the need for the legal regimes that the Principles contemplate. On the other hand, an attempt to narrow the definition of digital asset to exclude such digital assets might risk the exclusion of assets that would (or could) benefit from inclusion.

Discussion Questions:

1. Is the distinction between information that is or is not included in a digital asset accurately and adequately described in the foregoing commentary and illustrations?

2. Are there other illustrations that would be useful in explaining the concept of 'digital asset' and the scope of these Principles?

PRINCIPLE [X.1D]
Definition of 'control'

(1) A person has 'control' of a digital asset if:

(a) subject to paragraphs 2 and 3, the digital asset or the relevant protocol or system confers on the person:

(i) the exclusive ability to change the control of the digital asset to another person (a change of control);

(ii) the exclusive ability to prevent others from obtaining substantially all of the benefit from the digital asset; and

(iii) the ability to obtain substantially all the benefit from the digital asset; and

(b) the digital asset or its associated records allows)the person to identify itself as having the abilities mentioned in paragraph (1)(a).

(2) A change of control includes replacing, modifying, destroying, cancelling, or eliminating a digital asset and the resulting and corresponding derivative creation of a new digital asset (a derivative digital asset) and subjecting the derivative digital asset to the control of another person.
(3) An ability for purposes of paragraph 1(a) need not be exclusive if and to the extent that:

(a) the digital asset or the relevant protocol or system limits the use of or is programmed to make a change of control of the digital asset; or

(b) the person in control has agreed or consented to or acquiesced in sharing the ability with one or more other persons.

(4) In any proceeding in which a person's control of a digital asset is at issue, it is sufficient for that person to demonstrate that the identification requirement in paragraph (1)(b) is satisfied as to the abilities specified in paragraph 1(a)[(i) and (ii)]. It is not necessary for the person to prove the exclusivity of any ability specified in paragraph 1(a), i.e., that no person other than the person in control and those permitted by paragraph (3) has that ability.

(5) The identification mentioned in paragraph (1)(b) may be by a reasonable means such as (but not limited to) an identifying number, a cryptographic key, an office, or an account number, even if the identification does not indicate the name or identity of the person to be identified.

Key considerations in respect of this definition: Purpose and role of 'control'

- The exclusive ability requirements in paragraph (1)(a) of this Principle (as relaxed in paragraph (3)) recognize that the ability to exclude is an inherent aspect of proprietary rights (i.e., proprietary interests or rights with proprietary effects). These requirements contemplate that 'control' assumes a role that is a functional equivalent to that of 'possession' of movables. The exclusivity criterion of control (including the standards for its relaxation) appears to reflect the norm in the relevant markets for digital assets. Acquirers expect and believe that they have obtained the relevant exclusive abilities with respect to a digital asset (subject to understood exceptions) and in fact that generally has been the case.

- Because control assumes a role that is a functional equivalent to that of 'possession', a State may wish to consider using a term other than 'control' (e.g., 'possession') if necessary or helpful to accommodate other aspects of its legal system. However, 'possession' in this context is a purely factual matter and not a legal concept.

- The concept of control in a law governing digital assets serves as a necessary (but not a sufficient) criterion for qualifying for protection as an innocent acquirer of a digital asset (other than as a client in a custodial relationship) and as a method of third-party effectiveness (perfection) and a basis of priority of security rights in a digital asset. States also may choose to adopt the concept of control as an element of third-party effectiveness of proprietary interests more generally.

- The change of control from one person to another person must be distinguished from a transfer of proprietary rights. A change of control may or may not be associated with a transfer of proprietary rights. And a transfer of proprietary rights may or may not be accompanied by a change of control. This explanation reflects the understanding off the control of a digital asset as a functional equivalent of possession. In an effort to highlight this distinction between changes of control and transfers of proprietary rights, instead of references to, e.g., a 'transfer of control', a 'delivery', a 'delivery of control', or similar references, this Principle refers simply to a 'change of control'.

- The concept of control also may be relevant in the context of the custody of digital assets in an arrangement in which a custodian is to hold (ie, administer) digital assets for its clients. The private law (as well as a regulatory framework) may require a custodian to maintain control of digital assets held for clients. This is an example of one person (the custodian) having control while proprietary rights are transferred to or remain with another person (the client). A thief of digital assets would be another example of the separation of control and proprietary rights.

Explanation and commentary

'Ability' of a person with control

1. In this Principle the term 'ability' is used instead of the term 'power'. While the terms have identical meanings, 'ability' is more compatible with the concept of control as a factual standard

and 'power' has a more 'legal' connotation. On the exclusivity aspect of required abilities, see paragraphs [3-9], *infra*.

32. Paragraph (2) of this Principle addresses the situation in which the change of control relates to a derivative digital asset over which control is acquired, inasmuch as the derivative digital asset is not the same digital asset as to which control was relinquished. An example of such a derivative digital asset is the UTXO (unspent transaction output) generated by a transaction in Bitcoin. Another example might be adjustments in balances in accounts resulting from transactions in ether on the Ethereum platform, as to which control is relinquished and acquired over fungible assets that are not necessarily the "same" assets.

Exclusivity of abilities

3. The exclusive ability requirements in paragraph (1)(a) (as relaxed in paragraph (3)), as noted above, reflect the ability to exclude as an inherent attribute of proprietary rights. However, it is possible that a person (other than a person rightfully in control, and who has no proprietary rights) might acquire these abilities without the consent of the rightful control person, such as by the discovery of relevant private keys through "hacking," finding or stealing a device or other record on which the keys are stored, or otherwise. This underscores the distinction between a change in control and a transfer of proprietary rights.

4. Paragraph (3) provides explicit relaxation of the exclusivity requirements imposed by paragraph (1)(a). Paragraph (3)(a) contemplates situations in which the inherent attributes of a digital asset or the system in which it resides impose exceptions to the exclusivity of a control person's abilities. It recognizes that in many cases a person in control will not have abilities that actually are exclusive in a strict, literal sense. Subparagraph (b) recognizes that a person in control may wish to share its abilities with one or more other persons for purposes of convenience, security, or otherwise. For example, in a multi-signature (multi-sig) arrangement, if a person can identify itself under paragraph (1)(b) it could have control even if it shares the relevant abilities with another person. This is so even if the action of the other person is a condition for the exercise of a relevant ability. See Illustration 1, *infra.*

5. If a person were to obtain the relevant abilities without the consent of the rightful control person, then the rightful control person no longer would have control under the proposed criteria, the exclusivity having been compromised. However, that possibility should not provoke any practical concern or provide a basis for adjusting the exclusivity criterion. See paragraphs [7] and [8] *infra*.

6. Paragraph (1)(a)(iii) of this Principle does not require that the specified ability there must be exclusive. Inasmuch as a control person must have the exclusive ability to prevent others from obtaining substantially all of the benefit of a digital asset, it may be of no (legal) consequence that a control person has elected to permit another person (or persons) to obtain the benefit. It also may be that this situation is already covered by the exceptions provided in paragraph (3)(b), which permits sharing of abilities. If so, whether or not the ability specified in subparagraph (a)(iii) is required to be exclusive may be of little or no consequence. In any event, a control person need not prove a negative, as provided in paragraph (4) of the Principle and explained in paragraph [7], *infra.*

7. Only in a litigation context (broadly construed) would an issue arise as to which person has control of a digital asset under a digital assets law that includes the criteria specified by this Principle. If the control of a person is challenged it would be impossible for the putative control person to prove a negative—that no person other than one permitted by the definition has the relevant abilities. Paragraph (4) of the Principle makes it clear (although it would be implicit in any event) that a person asserting that it is in control of a digital asset meets its burdens of production and persuasion by showing that it has the specified abilities. It need not prove the negative—that no one else has the abilities—in order to prove that it has control. Of course, a person who was previously (rightfully) in control may demonstrate that it has a better proprietary interest than the person currently in control by proving that the change of control was wrongful.

8. As a practical matter, there is little chance that another person would appear in a contested proceeding to claim that it has the relevant exclusive abilities without the putative control person's consent. Under the criteria, that other person also would not have control. Any concern about such a person (e.g., hacker, thief, or finder) appearing to make such a claim seems unwarranted. Moreover, experience has shown that in situations in which the relevant abilities have been

obtained wrongfully the abilities have quickly been exercised and the assets have been removed from the control of the original control person. This reflects a set of risks that are inherent in digital assets.

Illustrations of the application of Principle X.1D (definition of 'control')

Illustration 1: Shared control and multi-sig arrangements.

Investor acquires proprietary rights in a digital asset (cryptocurrency) held in a public blockchain platform. Investor holds through a multi-sig arrangement in which the two of three private keys—the Investor's private key and the private keys of X and Y, parties trusted by Investor—are required to change control of the digital asset. Assuming Investor has all of the abilities specified in paragraph (1)(a) of the Principle and can identify itself as provided in paragraph (1)(b), Investor has control over the digital asset. Although Investor has shared the ability to change control specified in paragraph (1)(a)(i) and action by X or Y is a condition for Investor to exercise that ability, paragraph (3)(b) provides an exception to the exclusivity requirement of paragraph (1)(a)(i).

PRINCIPLE [X.2]
Acquisition and Disposition ('Transfer') of Digital Assets

(1) The applicable law other than law governing digital assets contemplated by these principles (ie, the digital assets law) should specify which (if any) of its existing rules or standards of general application govern the acquisition and disposition of proprietary rights in digital assets. (As used in these Principles references to proprietary rights include proprietary interests and rights with proprietary effects.)

(2) The law should provide that digital assets may be the subject of proprietary rights.

(3) The law should define the transfer of a digital asset as the change of a proprietary right from one person to another person and provide that a transfer includes the replacement, modification, destruction, cancellation, or elimination of a digital asset and the resulting and corresponding derivative creation and acquisition of a new digital asset (derivative digital asset).

(4) Except as otherwise provided in these Principles, the applicable law other than the digital assets law governs issues relating to proprietary rights, such as:

(a) whether a person has a proprietary right in a digital asset;

(b) whether a person has validly transferred a proprietary right in a digital asset to another person and the requirements for any such transfer;

(c) the rights as between a transferor and transferee of digital assets and derivative digital assets *inter se*; and

(d) the requirements for and legal consequences of a transfer of digital assets vis-à-vis third parties (ie, "third-party effectiveness").

(5) The law should [address][specify] the following aspects of the transfer of digital assets as between the transferor and transferee *inter se*:

(a) a "shelter" principle that would benefit (among other transferees) onward direct (ie, from an innocent acquirer to an initial transferee) and indirect (ie, from an initial transferee and onward) transferees from an acquirer protected by the innocent acquisition rule; and

(b) requirements for the creation of security rights.

(6) The law should [address][specify] the following aspects of third-party effectiveness:

(a) an innocent acquisition rule (IAR) that protects the rights of an innocent acquirer (IA) of digital assets, addressed in paragraph (8); and

(b) third-party effectiveness (perfection) [and priority] of security rights, addressed in [xr to relevant Principle(s)].

(7) The law should provide choice-of-law rules that address in general the law applicable to transfers of digital assets, including the rights of transferors and transferees *inter se* and third-party effectiveness.

(8) The law should specify the requirements for a transferee to qualify as an innocent acquirer (IA) of digital assets and derivative digital assets and the rights obtained by an IA (e.g., requirements and rights akin to those found in good faith purchase, finality, and take-free rules).

(a) The IAR should provide for strong and robust protection for IAs of digital assets to the end that IAs take digital assets and derivative digital assets free of conflicting proprietary rights (proprietary claims).

(b) The IAR also should provide that no rights based on a proprietary claim relating to a digital asset or derivative digital asset may be successfully asserted against an IA of that digital asset.

(c) "Control" of a digital asset or derivative digital asset should be an essential element for qualifying as an IA.

(d) As a corollary and necessary implication of subparagraph (c), an IA may acquire a proprietary right in a digital asset or derivative digital asset even if control of the IA is changed by a person that has no proprietary right in the digital asset and that is acting wrongfully.

(e) Concerning the test or standard for an IA's protection under an IAR, consideration should be given to (but not limited to) the following:

(i) an acquirer's possible notice or knowledge of any proprietary claim or of the specific proprietary claim at issue;

(ii) as to notice, an acquirer's reason to know of a proprietary claim or knowledge of suspicious circumstances and failure to investigate further;

(iii) as to knowledge, an acquirer's actual knowledge;

(iv) an acquirer's notice or knowledge that its acquisition [violates the rights of] [is wrongful as to] the holder of a proprietary claim;

(v) an acquirer's "good faith" (or a similar standard), taking into account the variety of meanings and interpretations under different legal traditions;

(vi) an acquirer's acquisition for value given by the acquirer or received by the transferor;

(vii) applicable tests or standards for the innocent acquisition protection for acquirers of movables and intangibles; and

(viii) the test adopted in the Geneva Securities Convention, Article 18(1), ie, whether:

> an acquirer actually knows or ought to know, at the relevant time, that another person has an interest in securities or intermediated securities and that the credit to the securities account of the acquirer, designating entry or interest granted to the acquirer violates the rights of that other person in relation to its interest.

(9) In the case of an IAR providing that qualification as an IA requires the absence of notice or knowledge, the law should specify the effect of a transferee's notice or knowledge, including its impact on the claims as to which a transferee does and does not take free (e.g., whether the notice or knowledge bars a transferee from IA status entirely or instead merely prevents an IA from taking free only of proprietary claims that are the subject of the notice or knowledge).

(10) The law should provide that a person (Client) that acquires a proprietary right in a digital asset through a custody relationship with a Custodian would take its right free of conflicting proprietary claims, or that no rights may be asserted against the Client based on a conflicting proprietary claim, or both, subject to substantially the same conditions that apply under the IAR (but without a requirement that the Client obtain control over the digital asset).

(11) The law should provide that that the digital assets law and the rights of an IA thereunder do not impair or affect the rights of any person under an adopting State's laws relating to intellectual property.[16]

(12) The law may, consistent with these Principles, address other issues relating to proprietary rights in digital assets.

Key considerations in respect of this Principle

- This Principle addresses several substantive provisions, such as innocent acquisition and the shelter principle. But it also is very much directed to the scope of the issues relating to proprietary rights in digital assets—ie, matters that are and that are not covered by the Principle—and thus to the scope of the digital assets law.

- References in this Principle to "the law" or to "the digital assets law" contemplate positive legal rules that would address specifically digital assets. However, this Principle takes no position as to whether those rules should be included in a special law on digital assets, incorporated into more general laws, or addressed by a combination of these approaches. References in this Principle to applicable law other than law governing digital assets contemplated by these Principles (ie, the digital assets law) are to laws of general application that do not address specifically digital assets.

Explanation and commentary

1. Paragraph (3) addresses not only the transfer of a digital asset from one person to another person but a transfer that results in the acquisition of a derivative digital asset that is not the same digital asset that was disposed of by the transferor. An example of such a derivative digital asset is the UTXO (unspent transaction output) generated by a transaction in Bitcoin. Another example might be adjustments in balances in accounts resulting from transactions in ether on the Ethereum platform, as to which the digital asset that is disposed of and the digital asset that is acquired are fungible assets and not necessarily the "same" asset.[17]

2. The deference to other law mentioned in subparagraph (a) of paragraph (4) is consistent, for example, with the approach in the Cape Town Convention, which defers to other law as to whether a person has a "power to dispose" of an interest in mobile equipment. The deference to other law mentioned in subparagraph (b) contemplates, for example, that a transfer may require an agreement or manifestation of intention by a transferor or that such an agreement might by itself result in a transfer of proprietary rights (whether or not limited in effect to the parties as contemplated by subparagraph (c) and subject to the digital assets law, including, but not limited to, paragraph 8(c)).

3. Paragraph (7) reflects the view that the law should provide choice-of-law rules relating to digital assets.[18]

4. The rights conferred on IAs in accordance with subparagraphs (a) and (b) of paragraph (8) mean that digital assets will have attributes similar to those of negotiability

[16] The substance of this provision may be relocated to a section of the Principles dealing with general provisions. The Working Group also way wish to consider whether the Principles should invite States to consider other potential conflicts between a digital assets law and other laws.

[17] This comment is similar to [Control] Principle X.1D, Explanation and commentary, paragraph 2. Ultimately the point of these comments might be made as a part of only one of the Principles with that Principle containing only a cross-reference to other relevant Principles.

[18] Subgroup 2 has not considered the content of any such rules, which have been the subject of discussion in Subgroup 4. Moreover, the substance of paragraph (7) might better be included within a set of Principles on choice of law more generally.

under rules applicable in some jurisdictions to negotiable instruments, negotiable documents of title, and negotiable certificated securities.

5. Subparagraph (d) of paragraph (8) is intended to make clear that, for example, even if an acquirer receives control of a digital asset by a change in control made by a thief or a hacker, the acquirer may qualify as an IA. See also the discussion in [Control] Principle X.1D, Explanation and commentary, paragraph 3.

6. Paragraph (10) is intended to confer on a Client in a custodial relationship substantially the same benefits conferred on an IA under the IAR. However, the doctrinal approach may be different in the case of a Client in a custodial relationship. For example, the Client's proprietary right may be in a fungible bulk of digital assets. Moreover, in a custodial relationship it would be the Custodian that would be in control of the relevant digital asset(s) and not the Client. Paragraph 10 should be coordinated with Principle[s][C]. [Note: Consideration should be given to a variety of contexts in which questions as to the nature and extent of propriety rights may arise in the context of custodial relationships.

Annex III – Appendix 2 – SUB-GROUP 2 – Control and Transfer

Sub-Appendix A

Discussion Questions: Principles on Scope, Definitions, and Controls

1. Scope

Our working assumption is that the scope of the project is the private law relating to digital assets—as will be defined in the Principles.

a. Is this approach acceptable?

2. Definition of "electronic record"

a. Should the definition of electronic record provide that it is limited to information (i) stored on a blockchain, (ii) stored in a system employing Distributed Ledger Technology, or (iii) stored in a system employing public key cryptography? Or should it remain technology neutral?

Note: The current draft is functional and technology neutral in that the definition of electronic record is not limited to information stored on blockchain or in a system employing Distributed Ledger Technology or to records or systems employing any particular technology.

b. Should the definition of electronic record or the related commentary make any reference to a connection with other assets (e.g., bank accounts, (intermediated) securities accounts, or negotiable instruments) recorded on an electronic ledger?

Note: Currently the definition simply refers to "information . . . stored," which is not limited to any particular type of information, including information related to other assets. But whether or not an electronic record has any relevance to rights or interests in any other property is dealt with in point 5, below, relating to "tethered" assets.

3. Definition of "digital asset"

a. Should the term "digital asset" be changed to "transferable digital asset", "controllable digital asset", or another term?

Note: The current draft uses "digital asset" to make these Principles intuitively understandable as well as for ease of use. Although the term is defined narrowly so that it means only a digital asset which is capable of being subject to control (as defined), digital asset is a broad term that may be misleading to some users of the Principles. "Transferable digital asset" would align with the term "electronic transferable record" as defined in Article 2 of the UNCITRAL Model Law, whilst "controllable electronic record" is used in the current draft UCC Article 12.

b. Should the commentary to these Principles explain more clearly that a "transfer of a digital asset" means the change of rights in the same digital asset in addition to explaining how a transferee may acquire a "derivative" digital asset (as per X.2(3))?

c. Should the commentary also elaborate on the distinction between a transfer of a copy of a digital asset and transfer of control of a digital asset?

4. Definition of "control"

a. Should the definition of control explicitly address both "positive" and "negative" control concepts, or should this be left to the explanatory comments and illustrations?

Note: The current draft contemplates both positive ([(1)(a)(i)] ability to change control and [(1)(a)(iii)], ability to obtain substantially all benefits) and negative [(1)(a)(ii) ability to prevent others from obtaining benefits] elements. In a "multi-sig" arrangement persons sharing control may each have negative control and none may alone have positive control.

b. Should the illustrations of digital assets that are capable of being subject to control be expanded? If so, what are some additional examples?

c. Should the illustrations of "shared control" be expanded beyond the "multi-sig" example in Illustration 1 to the definition of control? If so, what are some additional examples?

d. Should the definition of control explicitly include "derivative" control—i.e., that control could be achieved by a person if another person in control holds control on behalf of the person.

Note: As currently defined the concept of control is strictly factual — based on a person's possession of actual abilities in fact. Of course, a person may have control through an agent (and juridical persons can *only* act through agents). But the question asks whether one can have control through another person even in the absence of a formal agency relationship.

This concept of derivative control may be relevant in the context of sub-custodians and perfection of security rights. Another approach would be to recognize the effectiveness of such derivative control for purposes of, e.g., holding through a sub-custodian and perfection, without the beneficiary of another person's control being in actual control itself.

5. Principle(s) on "tethered" assets

a. Should the Principles explicitly address the potential role of digital assets in transferring rights in exogenous assets "tethered" to digital assets? If so, what should be the content of principle(s) relating to tethered assets?

b. Should the Principles provide that, whether the acquisition of a digital asset *ipso facto* results in rights in any other asset, will depend on the application of other law, including any relevant contractual arrangements, and the relevant facts?

c. Should the Principles instrument include commentary and illustrations of tethered assets? If so, what would be the best examples?

Appendix 3 – SUB-GROUP 3 – Secured transactions

Taking of security over digital assets

1. As part of the intersessional work that the Working Group agreed upon at its first session, Sub-Group 3 was set up to examine questions relating to secured transactions in the area of digital assets (a full list of the participants is available at **Annex 2, Appendix 3**). Led by Chair Marek Dubovec, the outcome of these meetings was the preparation of a list of issues together with several illustrations, special sections on digital twins and on decentralized finance (available below at **Sub-Appendix A**), a series of draft principles together with commentary, found below, for the consideration of the Working Group. The objective of this sub-group is to develop a principle on every aspect of a secured transaction – scope, creation, perfection, etc., and then consider where additional principles might be useful. The draft principles must be coordinated with the principles being developed by other sub-groups as well as other projects of UNIDROIT, particularly concerning effective enforcement. Sub-Group 3 identified the following as the primary sources of inspiration: i) the UNCITRAL Model Law on Secured Transactions; ii) the Geneva Securities Convention; and iii) the UNIDROIT Netting Principles.

2. At its previous sessions, the Working Group primarily focused on the use cases, illustrations, and draft Principles concerning certain aspects of secured transactions. The Working Group agreed that the Principles should be drafted in a legal system neutral language and should not reflect a particular approach to a secured transactions law (e.g., the functional approach where registration is the primary method of perfection). In addition to providing principles not reflective of a particular approach to secured transactions, attention has been paid to harmonizing the concepts and terminology used elsewhere in this project, particularly that of control, which may also function as a method of achieving third-party effectiveness for security rights.

3. Presently, the draft Principles concern digital assets that are not tethered to/embody another asset. Secured transactions laws provide for rules applicable to specific types of assets (e.g., negotiable documents, securities, etc.), but do not prescribe when an asset falls under a particular type (e.g., see the definition of negotiable document in the UNCITRAL Legislative Guide on Secured Transactions deferring to the law governing the document as to its negotiability). Accordingly, secured transactions laws do not create an asset that embodies another asset, but rather enable an asset of that nature recognised as such under the applicable law to be used as collateral (e.g., Article 16 of the UNCITRAL Model Law). If some other applicable law, whether statutory or judge-made law recognizing a particular practice, treats a document or record to embody an interest in some other asset, generally, under the secured transactions law a security right in that document/record would also extend to the associated/other asset. For a detailed explanation as to the processes how a document/record may be recognized as embodying rights/interests in some other asset see **Sub-Appendix A**.

4. States may, 1) be satisfied that their existing law already adequately supports the types of secured transactions involving digital assets common in the market; 2) amend their existing secured transactions laws, such as to include digital assets specific rules, or 3) enact digital assets specific statutes. In the last case, the State will need to consider various forms of interaction with the general secured transactions rules, such as where a sale of a digital asset generates a receivable. Article 1(4) of the UNCITRAL Model Law addresses one such type of interaction where a disposal of a movable asset generates proceeds of the type not covered thereunder. This Section of the Issues Paper does not attempt to anticipate what types of issues of interaction may arise in implementing legislation governing security rights in digital assets. Given the specific considerations that ought to be taken into account, States should ensure that any implementation produces a coherent legal framework, not only in the context of the secured transactions rules, but more broadly the rules that affect the rights of secured creditors, particularly in insolvency.

5. The secured transactions Principles are agnostic as to the structure and nature of the secured transactions regime. They should be implementable in States with a single comprehensive secured transactions law that covers all types of rights in movable assets that secure an obligation, similarly to the UNCITRAL Model Law, as well as in States that approach security rights differently. The Principles do not take a position about the ideal structure and nature of the secured transactions regime but highlight some aspects of the regimes that may be more conducive to secured transactions involving digital assets.

Use of Digital Assets in Collateralised Transactions [continuously updated]

6. Digital assets are already used as collateral in several types of transactions, and structures are being designed to enable their use in a growing variety of transactions. Since the Principles are to be forward-looking, throughout the Project it is necessary to examine various illustrations of existing and prospective use cases as they emerge. This Section provides concrete illustrations to aid the discussion of the draft Principles. Some of these illustrations may cover transactions that are not commonly understood as creating rights in movable property to secure an obligation, but rather which mimic those structures and relationships. Even though they may generally fall outside the scope of secured transactions laws, given that they provide recourse against some asset, examining their mechanics and processes facilitates considerations as to whether any aspects of these transactions concern security rights, broadly understood, and how they interact with other relevant laws.

Illustration 1: Digital Assets "Securing" a Stablecoin

> The MakerDao system is an online service provider using smart contracts deployed on the Ethereum blockchain, allowing users to create structures that function like collateral transactions. Users surrender control of digital assets that are used as "collateral" by the system. Transfer of control occurs in a manner consistent with Principle X. In exchange, users receive access to an amount of a system-generated stablecoin (i.e., a cryptocurrency designed to minimize the volatility of the price of the stablecoin).[19] The system-generated stablecoins are, by design, intended to be always over-collateralized (i.e., the value of the deposited digital assets exceeds the value of the stablecoin) and resemble loans of property or commodity swap transactions. If the ratio of the value of the stablecoin to the value of the collateral reaches a limit, the collateral can be liquidated using a semi-automated process. A user can also provide an amount of the stablecoin back to the system to avoid liquidation of or to reclaim their "collateral". The system's smart contracts automate almost all functionality required to use the system, which does not require an identifiable counterparty to function, and allows the user to obtain a liquid asset while maintaining market exposure. The user who gives collateral and gets a stablecoin is not necessarily transacting with another legal entity – rather, it is using an appliance or service that is not owned managed or operated by any identifiable party. No legal contracts or legal compliance are included in the system or required to use the system.[20] No traditional intermediaries are involved in the operation of the system.

Illustration 2: Borrowing of Digital Assets

> Certain systems relying on smart contracts may create structures that are similar to lending. In these systems, participants may "borrow" digital assets from one another and promise to pay those users a yield (sometimes in kind, sometimes in fiat) for the use of their digital assets. Multiple centralized and decentralized platforms offer various types of "lending" to holders of digital assets. Participants surrender control of those digital assets in a manner consistent with Principle X and allow them to be lent or rehypothecated to others in an effort to earn yields that exceed the yields promised to be paid to participating users. Although structures and specifics vary based on the implementation, in the case of systems that include rehypothecation, the participant who makes their digital assets available to be used transfers control of those assets to the system operator, which may be a legal entity or smart contract code. While the system rules refer to lending and re-

[19] A stablecoin can be pegged to a cryptocurrency, fiat money, or to exchange-traded commodities (such as precious metals or industrial metals).

[20] There are terms of use that govern use of front ends and that in some cases protect the "maker dao volunteers" but those terms are not the agreements that are typical of these sorts of transactions as we generally understand them. For instance: https://vote.makerdao.com/terms.

hypothecation, the transactions are more akin to deposits in the search of a higher yield rather than transfers of digital assets to secure an obligation.

Illustration 3: Purchasing cryptocurrencies on margin

An exchange that facilitates selling and buying of virtual currencies may allow users to purchase virtual currencies on margin. If a person wishes to purchase $10,000 worth of Bitcoin but only has $5,000 available, the exchange may extend a $5,000 loan. The loan may also be extended in virtual currency where it is used to acquire another digital asset. The borrower will need to maintain sufficient collateral to cover maintenance margin requirements and top up the collateral if the Bitcoin value reduces to preclude the liquidation of the collateral. The Bitcoin may be held in a custodial wallet, liquidity pool or an account, and the ability of the borrower to transfer by sending an instruction to the exchange will depend on the terms of the security agreement.

Illustration 4: Central Bank Digital Currencies

A central bank digital currency (CBDC) may be issued by a central bank using a blockchain or other technology. A CBDC may be token or account based. It may require a supporting infrastructure where the CBDC, though issued by the central bank, is held by financial institutions for their customers similarly to deposit accounts. It may be used in a secured transaction either as original collateral or it may constitute proceeds of some other collateral where a security right is made effective against third parties by control. For instance, a financial institution that maintains a "CBDC account" for its customer extends a loan that is secured with the CBDC credited to that account over which the financial institution has control. For token-based CBDC not held in an account, the financial institution may acquire control over the CBDC token itself pursuant to Principle X. Although many States are currently experimenting with CBDCs and a few have launched them, presently there is no consensus or universal approach to the structure, design or use of these digital assets.

Illustration 5: Securing Exposures in Derivatives

A derivative is a contract the value of which is dependent on the value of another asset, such as a commodity. While derivative contracts may call for delivery of a digital asset like a virtual currency, rights in digital assets may secure the respective obligations of parties to a derivative. The potential use cases for digital assets in these transactions are only just emerging.[21] One of the main reasons why digital assets are not yet commonly used as collateral in these transactions is due to a lack of legal and regulatory certainty surrounding their use, a lack of common documentation standards, and insufficient digitization and automation of collateral processes. In addition, the volatility of some digital assets will likely continue to have a discouraging effect on their use within collateral management.

Secured Transactions Principles

Principle A: Secured transaction law applies to digital assets

1.The law should establish simple and sound rules in relation to collateral transactions involving digital assets.

[21] See International Swaps and Derivatives Association (ISDA) *Legal Guidelines for Smart Derivatives Contracts: Introduction* (Jan 2019), ISDA *Legal Guidelines for Smart Derivatives Contracts: Collateral* (Sep 2019), and ISDA *Private International Law Aspects of Smart Derivatives Contracts Utilizing Distributed Ledger Technology: Japanese Law* (Oct 2020) 14-16.

Comments:

While the content of this Principle is generally applicable to digital assets law, its inclusion for secured transactions specifically allows explanation of the key features of the laws governing the use of digital assets as collateral. In this Principle, the reference to "law" should be understood to include a general secured transactions law, a statute specific to creating interests in intangible assets, case law, or some combination of the preceding. If multiple laws provide for security devices that may be applied in secured transactions involving intangible assets, the State should decide whether to make all or some of them applicable to digital assets. If digital assets may be used as collateral under multiple security devices, the State should ensure that a coordinated and clear priority rule is provided for.

In this Principle, the reference to secured transactions should be understood to include various types of "security rights", such as pledges, charges, or security assignments. It also covers outright transfers where those might be used with respect to certain types of digital assets, such as those that are functional equivalents of receivables and serve to provide financing to the transferor. The UNCITRAL Model Law applies to outright transfers of receivables. The Geneva Securities Convention covers collateral transactions that are created by the grant of an interest in intermediated securities in the form of security interests and title transfer collateral agreements. Some domestic laws provide for fiduciary transfers of ownership that transfer "ownership" of the asset to the creditor with the sole purpose of securing an obligation. Finally, the secured transactions law should be coordinated with the generally applicable rules governing outright transfers of digital assets.

Illustrations:

A security right is taken in virtual currency, and the borrower delivers possession of a hard drive with access credentials that allow the user to transfer the virtual currency. It is unlikely that the delivery of the hard drive with access credentials would be classified as a traditional possessory pledge that has been applied to tangible assets only, and thus the security right would not be effective against third parties because the real value is the data on the hard drive.

A security right is taken over receivables and a bank account of a business. The secured creditor registers a notice describing the collateral as "all current and future receivables and bank accounts". The business borrower generates receivables that are payable in CBDC that are collected and deposited into an account maintained by a financial institution. In this situation, it may be unclear whether the account that holds the CBDC is a bank account that falls within the specific definition included in the applicable secured transactions law.

Notes:

Domestic laws may recognise a single (unitary concept) or multiple security devices that may be used to secure obligations. Some of these laws may provide for limitations that would exclude the use of digital assets, while some are sufficiently broad to enable collateralisation of any intangible assets. Nonetheless, many existing security devices are outdated so a legislative action to clarify their application to digital assets may enhance certainty.[22]

The applicable secured transactions law may not have a universally recognised definition/concept of security right. Certain types of security may be taken only over specific types of asset. For instance, due to the delivery-of-possession requirement, intangibles, other than those embodied in a negotiable document of title, instrument or

[22] For instance, the South African law provides for a notarial bond, cession *in securitatem debiti,* and a pledge. The notarial bond does not provide adequate protection due to the challenges with perfection.

security, may not be pledged by possession.[23] In other States, it is unclear whether the courts would recognise some form of equivalent to delivery such as by control of a digital asset (see Principle D) as a functional equivalent to delivering a tangible object under a pledge. Yet, in another group of States, the pledge may extend to intangible assets that is effectuated by assignment in security.[24]

Principle B: Digital assets are eligible to be collateral

1.The secured transactions law should make it possible to use any digital assets as collateral.

2.References in secured transactions laws to movable assets, personal property or any similar notion should be understood to include digital assets.

Comments:

Secured transactions regimes should enable the use of anything that is a movable asset and not necessarily property in the strict sense or capable of being controlled or maintained by a custodian as collateral. This approach allows prospective secured creditors to decide for themselves which of the digital assets of a loan applicant have any collateral value. This Principle builds on the Transfer Principle X.2(2) stating that law should provide that digital assets may be the subject of proprietary rights. The inclusion of Principle B.2 allows the explanation of this aspect in the context of secured transactions. Other law determines whether a digital asset embodies a right in another (tethered) asset.

Illustrations:

A security right may be taken over things, which are defined in the civil law of the State. It is unclear whether the definition of things would include digital assets.

A security right in a digital asset would not necessarily extend to any tethered asset unless the applicable law provides so. For instance, taking control over an electronic invoice by a factoring company would create and make a security right effective against third parties in the underlying right to payment only if the applicable law treats the invoice as an embodiment of the underlying right to payment. If the factoring company regularly takes possession of invoices for due diligence purposes, acquiring control over digital equivalents of invoices would not make the security right in the receivable effective against third parties.

Notes:

Some secured transactions regimes may enable the use of any movable property as collateral, while others specify the types of property that may be encumbered (e.g., equipment, but not inventory of a business, may be subject to an enterprise charge under some laws). The former, whether statutory or judge-made, may define a security right

[23] In the absence of special statutory provisions [e.g., Financial Collateral Arrangements Regulations SI 2003/3226, regulation 3(2)], possession cannot be taken over an intangible; 6OBG Ltd v Allan [2007] UKHL 21; Your Response Ltd v Datateam Business Media Ltd [2014] EWCA Civ 281. For German law, see Bürgerliches Gesetzbuch – BGB (German Civil Code), s. 90.

[24] BGB s.1273 et seq., 398, 413; G. McCormack, R. Bork, *Security rights and the European Insolvency Regulation* (Intersentia, 2017) 313. See also Code civil (French Civil Code), Articles 2355-2366; W. Faber, B. Lurger, *National Reports on the Transfer of Movables in Europe* (European law publishers, vol. 4). French law explicitly permits the creation of pledge ('nantissement') over incorporeal movable goods ('biens'), i.e., assets, either actual or future.

as a "property right in a movable asset", without defining "movable asset".[25] Applicable law defines what constitutes a movable asset. Some laws allow the creation of an interest with respect to anything that can be traded, including intangible assets.[26] Although actions, claims or rights may be listed as an example of an incorporeal asset in the relevant statutory provision, typically it is not clear whether digital assets would be covered. In principle, under these regimes, an interest may be created in any incorporeal asset, including digital assets. However, an explicit statutory treatment would in this case provide greater legal certainty.

Questions to the Working Group:

Do we need a separate principle that establishes how a security right created in a digital asset affects any tethered asset (see the second illustration about the invoice)? Guidance may be drawn from Article 16 of the UNCITRAL Model Law which provides that a security right extends to an asset covered by a negotiable document of title. In contrast, Article 17 provides that a security right in a tangible asset does not extend to any "associated" intellectual property. The "invoice illustration" is more akin to the approach of Article 17.

Should this Principle also address the converse situation where a security right is taken in the tethered asset and its effect on the digital asset (see again Article 17 of the UNCITRAL Model Law)?

Principle C: Distinct rules for different categories of digital assets apply to some aspects of creation of a security right and effectiveness against third parties

1.The law should provide for one or more types of digital assets where their individual features and characteristics are such that the application of specific rules, distinct from those applying to intangible assets generally, would be necessary. If the functions and features of various digital assets are substantially the same, a single type may suffice.

2.Separation of digital assets from the general category of intangible assets would enable the State to consider specific approaches, such as third-party effectiveness by control.

Comments:

Digital assets may fall under different types of collateral (e.g., securities, bank accounts, etc.) defined in the secured transactions laws. Depending on their characteristics, they may be treated as securities, funds credited to bank accounts, negotiable documents/instruments, if the State recognizes electronic documents and instruments, or fall under the residual category of intangible assets/general intangibles. As a consequence, the secured transactions rules specific to that type of asset will apply. A number of these rules have been designed with reference to the specific nature of an asset or the structure of the system in which it is transacted, which could cause challenges in determining how those rules are to be applied to security rights in digital assets. If a digital asset tethered to some real-world asset is recognized under some other law as a negotiable document, the creation and third-party effectiveness of a security right in the digital asset would extend to the real-world asset. Otherwise, the creation and third-party effectiveness of a security right would cover the digital asset only.

[25] This is the case of the UNCITRAL Model Law that also takes a comprehensive approach with the aim to cover all types of movable assets except those explicitly excluded (see article 1(3)). See also R. Goode, L. Gullifer, *Goode and Gullifer on Legal Problems of Credit and Security*, (Sweet & Maxwell, 6th edn, 2018) 39; G. McCormack, R. Bork, *Security rights and the European Insolvency Regulation* (Intersentia, 2017) 313.

[26] This would be the case of hypothecation under the South African law. See Voet *Commentarius ad Pandectas* 20.3.1; Digest 20.1.9.1 and 20.3.1.2.

States should consider providing for digital assets-specific rules. These rules may be made applicable to digital assets as a type of collateral or further distinctions made for various categories of digital assets (e.g., Bitcoin as contrasted from CBDC). There are advantages and disadvantages to both approaches, such as that the digital assets covered under a single type are so diverse that the uniform application of all rules may cause uncertainty. An advantage would be continuous coverage by the same set of rules in case the digital asset changes its inherent characteristics, such as the case in which a digital asset designed initially as a "utility token" subsequently acquires some features of a "security token". States should not attempt to provide for secured transactions rules specific to many categories of digital assets that would result in a complicated system.

Illustrations:

The secured transactions law does not carve out digital assets from the broader type of intangible assets. Control agreement is a recognized perfection mechanism, but available only for bank accounts and intermediated securities. The secured creditor may thus need to register a notice to perfect its security right, since a control agreement that it may have entered into with a custodian would not render the security right effective against third parties. The registration would be a redundant step in terms of providing public notice to third parties as the grantor would no longer retain any ability to dispose of the digital asset.

Principle D: Security rights may be made effective against third parties by control

1.The law should recognize control as a mechanism to achieve third-party effectiveness of a security right in a digital asset.

2.The requirements to achieve third-party effectiveness of a security right by control should reflect those set out in Principle X.

3.The law should specify which (if any) of its existing special rules govern the third-party effectiveness of security rights in digital assets.

Comments:

Third-party effectiveness generally requires a secured creditor to take a step to publicize its security right, which may include delivery of possession (pledge), notification of the obligor (security assignment), registration (floating charge), and control (security right). Some of these mechanisms may not be applicable to digital assets (e.g., delivery of possession of a tangible object) while others apply only to certain types of assets (e.g., control over bank and securities accounts). Some States recognize steps, such as "freezing" or "blocking" an asset in favor of the secured creditor that functionally achieve the same result as delivery of possession, as a mechanism to make the security right effective against third parties.

While in some States registration of a notice would generally render a security right in most (or all) types of assets effective against third parties, registrations are not commonly effectuated in the crypto-lending market, leaving some credit risk in the transaction. Furthermore, in States that do not have a registration system, market participants may not be aware of the existing requirements for third-party effectiveness or such requirements may be an obstacle to the practices.

Market participants generally take some steps to preclude the borrower from accessing the encumbered digital asset, typically by transferring it from the wallet of a borrower to a wallet, or under the control (e.g., in a multi-signature arrangement), of the secured creditor. Under some laws those steps may be recognized as a mechanism to make the security rights effective against third parties. A transfer to a wallet held by the secured creditor or its agent should be sufficient to protect the security right against third-party claims, including in insolvency. For instance, a security transfer of ownership may be effective against third parties upon executing of an agreement to that effect. For digital assets that may be encumbered under this device, the creditor might not need to take any additional step to make its security right effective against third parties. In contrast, in some regimes the failure to register a notice may be fatal for the secured creditor, as no other mechanism might exist to achieve third-party effectiveness of a security right in a digital asset. In any case, the existing requirements for third-party effectiveness create uncertainty for market participants.

Secured transactions and related laws may already provide for control over an asset that may effectuate its transfer, whether outright or as security. Control may be established through i) execution of a control agreement if the relevant asset is held with an intermediary (e.g., under the Geneva Securities Convention); ii) the mere fact that the secured creditor is the intermediary/deposit-taking institution itself (e.g., the UNCITRAL Model Law on Secured Transactions); or iii) applying a reliable method to establish exclusive control of an identifiable person (e.g., the UNCITRAL Model Law on Electronic Transferable Records). Where laws already recognize some form of control over specified types of movable assets, security rights in digital assets that would fall under that type of a movable asset could be made effective against third parties by control. This may be the case of virtual currency and "security tokens" that may be credited to bank and securities accounts, respectively. However, there are many other types of digital assets [reference to the taxonomy to be inserted later] for which control mechanisms have not been provided for.

Regimes governing security rights in certain types of assets have been amended reflecting the emerging industry practice (e.g., book entries to securities accounts in which financial collateral is held). The emerging practices in "crypto-lending" do not rely on registration and other traditional methods of achieving third-party effectiveness. States should incorporate "control" as defined in Principle X in their secured transactions laws to allow secured creditors to make their security right in digital assets effectiveness against third parties. Incorporation of control may affect the structure of its priority rules, which is explored below in Principle E on priority.

There are four situations in which control may be deployed to make the security right effective against third parties. First, the existing rules on control in the relevant secured transactions regime may be used if the digital asset qualifies as a particular type of asset (e.g., bank account). Second, the secured creditor may acquire the requisite powers prescribed in Principle X. Third, the secured creditor may share these powers with other parties, which would constitute control under Principle X. Fourth, a party that is currently in control (e.g., a custodian) may agree to exercise those powers on behalf of the secured creditor.

States should include a specific definition of control (or refer to such a definition included elsewhere in the digital assets law) to achieve third-party effectiveness conditioned on the secured creditor acquiring a set of abilities with respect to the digital asset. This project has developed Principle X on control that is suitable to achieve third-party effectiveness of security rights over any digital assets by transferring the powers specified therein to the secured creditor. The secured creditor may exercise the requisite powers directly, through an agent or in cooperation with other parties, such as in (a multi-sig) arrangement.

Although specific rules may have already been provided prescribing control for some assets, such as electronic transferable records, States should ensure that the existing criteria are sufficient to accommodate collateralization of these records issued and transferred in blockchain. For instance, the UNCITRAL Model Law on Electronic Transferable Records in Article 11 provides for control requiring that an identified person acquires exclusive control by a reliable method. States implementing this Model Law should consider incorporating the criteria establishing control under Principle X for transfers of "electronic transferable records", including achieving third-party effectiveness of a security right.

Illustrations:

A secured creditor takes a non-possessory pledge over a portfolio of virtual currency. The applicable law does not provide a specific mechanism to make a security right effective against third parties with respect to digital assets but provides that registration is the sole mechanism to achieve third-party effectiveness over any intangible assets provided as collateral. The secured creditor has its borrower transfer the relevant virtual currency to a third-party wallet controlled by the secured creditor through a multi-signature arrangement but does not effectuate a registration. Later, the borrower files for insolvency and the secured creditor could lose its security right as it was not made effective against third parties.

Digital assets are held by a custodian on behalf of a customer. The custodian undertakes to exercise the control abilities on behalf of the secured creditor upon receiving an instruction or the occurrence of some event. If the State has incorporated "control" as a method of third-party effectiveness in its secured transactions regime, the security right will be effective against third parties.

Principle E: Priority of security rights in digital assets made effective against third parties by control

1.The law should provide that where a security right in a digital asset has obtained third-party effectiveness through control, the security right should have priority over a security right in the digital asset of a person who does not have control.

2.Where more than one security right in the same digital asset has been made effective against third parties by control, priority should be based on the temporal order of obtaining control.

Comments:

Generally, the priority among competing security rights in the same asset is determined based on the temporal order of when the security right was made effective against third parties (for example, the order of registration). However, the law may grant priority to security rights in certain encumbered assets that are made effective against third parties by using a specific method for obtaining third-party effectiveness. For example, a security right in a negotiable instrument that has been made effective against third parties by possession typically has priority over other security rights made effective against third parties by other means. Similarly, there could be asset-specific priority rules for bank accounts, intermediated and non-intermediated securities, money, negotiable documents, and other types of assets. The relevant law has conferred some degree of transferability, typically negotiability, on these assets that also allows transferees to cut off security rights made effective against third parties by registration.

Providing for the non-temporal priority recognizes that the secured creditor that took the additional steps was relying to a greater extent on the encumbered asset. This approach also reflects the lending practice ("margin lending") where creditors may extend credit to their clients to enable them to acquire a digital asset with respect to which they expect to have priority over an earlier-in-time registration.

Similar concepts would apply to a security right in a digital asset. Where one secured creditor made its security right effective against third parties by registration or another mechanism recognized by the applicable law and another secured creditor made its security right effective by control (as defined under Principle Y), the latter would have priority even if it took the steps to obtain control after the former registered a notice relating to a security right in the registry or otherwise made it effective against third parties. This approach is consistent with the secured transactions rules, including the UNCITRAL Model Law and the relevant provisions of the Geneva Securities Convention that give priority to secured creditors that acquired some form of control over the collateral. A different approach would create distinctions between non-digital assets, such as funds held in deposit accounts, and their digital functional equivalents, such as the CBDC. Furthermore, Principle X.2(8a) on transfers generally cuts off any conflicting proprietary claims. The secured creditor acquiring control is expected to satisfy the other requirements to qualify as an innocent acquirer.

For assets that are not highly transferable such as equipment, the general priority rule of first-in-time applies. States may wish to consider whether security rights in certain types of digital assets should be made subject to the general priority rule.

Under Principle X, more than one secured creditor can obtain control (or share such ability) over the digital assets, which includes making their security right effective against third parties. As a result, there should be a rule to determine the priority between the multiple secured creditors based on the temporal order of obtaining control.

Illustrations:

A security right is made effective against third parties by registration in all assets of the borrower. Upon disposal of encumbered inventory, virtual currency is collected by the borrower and deposited with a custodian that also has control over the virtual currency. The custodian also extends a loan to the borrower that is secured with all virtual currency under its control. The security right of the custodian has priority over the security right in the virtual currency claimed as proceeds of the inventory, assuming the secured transaction system recognises control as a method of obtaining effectiveness against third parties, and gives a special priority to a security right made effective against third parties by control.

Principle F: Effective Enforcement of Security Rights in Digital Assets

1. The law should allow secured creditors to enforce their security rights in digital assets in a simple and quick manner. To that end, the law should not impose undue formalities or requirements that would make the enforcement process cumbersome.

2. The interests of third parties, particularly custodians should be protected.

3. Given the nature of digital assets, the law should recognize that enforcement actions may be taken automatically and that some requirements for enforcement, such as to provide a notification of disposal, should not apply.

Comments:

This Principle concerns legal rules governing enforcement of security rights rather than technologies that may facilitate the enforcement of security rights in general (e.g., locating and remotely disabling the collateral). This Principle does not concern judicial enforcement that may need to be resorted to when extra-judicial remedies are unavailable/unenforceable. These and other aspects regarding effective enforcement are explored in another project of UNIDROIT: *Enforcement: Best Practices* - https://www.unidroit.org/work-in-progress/enforcement-best-practices/.

The law should not preclude secured creditors from exercising remedies that may exist under other laws or have been provided for in the security agreement. When digital assets become widely used in securities transactions, derivatives, and similar financial structures, States should ensure that close-out netting is available to parties to such transactions.

All enforcement actions, including disposal, collection of payment (if monetary obligation is the main characteristic of a digital asset) and acceptance of the collateral, in full or partial satisfaction of the secured obligation, should be available. In enforcing their rights, secured creditors must proceed in a commercially reasonable manner and satisfy certain conditions that balance the interest of affected third parties. The inherent design of the digital asset may prevent exercising certain enforcement rights. General rules governing enforcement, typically included in international standards on secured transactions appear to be flexible enough to accommodate the expectation of digital assets lenders and other relevant parties. However, States should take into account several considerations.

First, enforcement rules empower a secured creditor to take a post-default action. Generally, a secured creditor or its agent would take some action, such as repossessing the collateral or instructing the debtor of a receivable to pay to a different bank account. While the rules focus on post-default actions taken by secured creditors, they should not render a "pre-programmed action" that occurs automatically, such as causing liquidation of the digital asset when the collateral-to-loan ratio falls under a specified threshold ineffective. See Illustration 1 above for the automated enforcement action occurring upon reaching a specific collateral-to-value limit.

Second, secured transactions laws balance the interest of affected parties by imposing certain requirements on secured creditors, such as to provide notifications. However, under certain situation these requirements may not apply. For instance, Article 78(8) of the UNCITRAL Model Law provides for exceptions from the requirement to provide a notification when the asset may speedily decline in value or is sold on a recognized market. These kinds of exceptions should arguably apply to many digital assets (e.g., Bitcoin may speedily decline in value while stablecoins may not, and some NFTs may already trade on recognized markets while others do not). Enforcement provisions in secured transactions laws may not need to be changed to accommodate digital assets as these exceptions were generally crafted broadly to accommodate future developments. For those digital assets that qualify as intermediated securities (e.g., upon their credit to a securities account), any notification requirements may not apply at all (see Article 33(3)(a) of the Geneva Securities Convention).

Third, States should be mindful of some limitations on the enforcement rights. One such limitation relates to the mechanism used to make the security right effective against third parties, which can have an impact on the ability to enforce security rights. For instance, the law should provide that if the secured creditor registered a notice, secured creditors may not be able to extra-judicially enforce their security rights in digital assets held with custodians. This approach mirrors the rules that protect intermediaries, such as banks against "unknown" third-party creditors. Extra-judicial enforcement is available when the secured creditor holds a power to instruct the custodian to change control of a digital asset or have entered into a control agreement with the custodian (see Article 82(4) of the UNCITRAL Model Law). In other words, control is the facilitator of enforcement upon default.

Fourth, collateral may need to be disposed of in a public/private sale that proceeds differently from selling tangible collateral, for instance. Smart contracts may execute successive auctions of the encumbered digital assets until the secured obligation is satisfied. Thus, the collateral may not be sold in its entirety, and any collateral in excess of the amount necessary to satisfy the secured obligation is returned to the borrower. The law should not preclude such automatic liquidation of the collateral or impose requirements before each of the successive auctions can proceed.

Illustrations:

A security right was made effective against third parties by control where the secured creditor is one of the three parties to a multi-signature arrangement. While the grantor is also a party to this arrangement, the third person acts on behalf of the secured creditor. Upon default, the multi-signature arrangement is triggered, and the encumbered digital asset is transferred under the "sole" control of the secured creditor resulting in the acceptance of the collateral in satisfaction of the secured obligation or enabling a foreclosure sale.

Upon default, the ability of the secured creditor to dispose of the digital asset in a public auction may be affected by the design of the digital asset that may preclude its transfer out of the system in which it was issued and trades.

Questions to the Working Group:

Does the draft Principle adequately cover the aspects relevant to enforcement of security rights in digital assets?

Should additional aspects be covered?

Principle G: Insolvency law should recognize the third-party effectiveness and priority of security rights established prior to the opening of insolvency proceedings

1.The law should specify that where a security right in a digital asset is effective against third parties under the applicable secured transactions law, it will be recognized as effective against the insolvency administrator and competing claimants in any insolvency proceeding.

2.The priority of a security right in digital assets established under the applicable law should be the same, except if, pursuant to insolvency law, another claim is given priority.
3.Secured creditors should be entitled to claim the value of encumbered digital assets.

Comments:

The insolvency law should recognise the third-party effectiveness and priority of a security right and should not impair it for the sole reason that the collateral is a digital asset. The insolvency law should not impose any further requirement to establish or maintain the third-party effectiveness of a security right established prior to the insolvency proceedings (see Art. 11(2) of the Geneva Securities Convention).

The insolvency law should also respect the pre-commencement priority of a security right in a digital asset, subject to any "preferential claims" under insolvency law. Any rules on the (a) priority of claims; (b) avoidance actions and (c) the limitations on the enforcement of security rights in property that is under the control or supervision of the insolvency administrator shall not be affected.

Determining whether, and to what extent, a secured creditor is actually secured and may claim the value of its security right, requires valuation of the encumbered digital asset. Insolvency law may require/allow valuation of an encumbered asset pursuant to a pre-petition agreement of the parties, by the insolvency representative or by the court on the basis of evidence, including market considerations and expert testimony, taking into account the purpose of the valuation. The established insolvency law mechanisms for ascertaining the value of the asset may reflect either the going concern value or liquidation value. The relevant valuation date is crucial. This means that there may be a need for an ongoing valuation at different stages of the insolvency proceedings in order to determine the value of the encumbered asset itself, including facilitating the distribution of the proceeds of sale of the encumbered asset. Alternatively, upon commencement, the encumbered asset is valued and the amount of the secured portion of the creditor's claim is determined immediately, remaining unaffected in the course of the insolvency proceedings. In order to provide adequate protection of the security right in a digital asset in the insolvency proceedings and preserve the value of a creditor's security right, the valuation of the encumbered asset should take into account the high volatility and sharp fluctuations in value of many digital assets.

Valuation of assets affects recovery of secured creditors in an insolvency proceeding. It also impacts other aspects of secured transactions, including determination of the amount to be lent and distribution of proceeds upon disposition of the collateral. Insolvency laws do not provide specific guidance on the valuation method to be used, such as the "going concern value" or the "liquidation value". Currently, there are no standardized valuation approaches which creates uncertainty for secured creditors as to the value they may be able to receive. Given these challenges, it might be useful to explore and assess whether and how the existing valuation standards and methods apply to digital assets,[27] focusing on the rights of secured creditors in insolvency. This may be particularly necessary for digital assets that do not have a value that may be readily established for instance through a secondary market. Such assets may include some NFTs and utility tokens, the value of which is not necessarily determined by supply and demand and thus, may require different ways to measure the value; for instance, by comparing them to similar ones. Valuation of "digital twins" may present peculiar challenges as well. The international standards could offer guidance as to which valuation approaches and methods to apply to digital assets, in accordance with their classification. On the contrary, valuation of digital assets, such as CBDCs, stablecoins, and other virtual currencies might be more straightforward but it could still benefit from further guidance.
Considering the diversity of rights and obligations associated with digital assets, the choice of the valuation approach may highly depend on the classification of the digital asset and its intended purpose. Besides, different valuation approaches may provide different results as the inputs used may vary. In specific circumstances involving certain digital assets, one valuation approach may be more appropriate than the others. Methodologies for the valuation of digital assets started to

[27] Relevant international standards would include the *International Valuation Standards (IVS)* produced by the International Valuation Standards Council (IVSC), and the *International Financial Reporting Standards (IFRS)* developed by the International Financial Reporting Standards (IFRS) Foundation mainly through its standard-setting body, the International Accounting Standards Board (IASB).

emerge, drawing on those applicable to intellectual property.[28] This is particularly relevant for those digital assets linked to an intellectual property right (e.g. NFTs associated with art).

In addition, due to the high volatility and uncertainty surrounding the value of many digital assets, the valuation date may be crucial to determine the value of the secured claim. Further guidance on how to choose the valuation date might be necessary in light of the high volatility of some digital assets.

A further issue concerns whether valuation, and consequently distribution, should take place in fiat or virtual currency. For instance, in an insolvency scenario where digital assets are valued and converted to fiat currency, creditors may receive the cash value of the assets, but would lose any future appreciation that the digital assets might accrue.

Illustrations:

A security right in a digital asset is granted to a lender, and later the borrower becomes subject to an insolvency proceeding. The insolvency administrator claims that the digital asset is not property, and thus a security right has not been created, or otherwise challenges the third-party effectiveness of a security right beyond the parameters set out in the applicable secured transactions law.

The insolvency law requires the valuation to refer to the effective date of commencement of insolvency proceedings. The insolvency representative administering the insolvency proceedings values the secured creditor's claim based upon the market price of the digital asset at the time of the commencement of the proceedings, which is substantially lower than the value at the time of a distribution.

Questions to the Working Group:

> Bearing in mind the prevailing view that this Project should not explore general aspects of insolvency, some aspects of custodian insolvency covered in the relevant custody principles, and some aspects of the applicable law covered in the relevant principles, are there any aspects directly connected to security rights that should be covered in this Principle?
>
> One example might be the application of the automatic stay in case the system is programmed to liquidate the collateral automatically. How should the insolvency law address these situations? Another example may be the treatment of proceeds where the insolvency law may confer a different treatment to cash and non-cash proceeds.
>
> The Working Group may wish to consider a number of issues related to valuation of digital assets, potentially expanding this principle on insolvency:
>
> > Exploring the existing valuation methods with the aim to provide guidance to secured creditors in insolvency and enforcement.
> >
> > Exploring the issue of proper timing for valuation (guidance on when to evaluate).
> >
> > Offering guidance on whether valuation (and distribution) should take place in fiat currency or virtual currency.

[28] A few reports on the analysis of suitable valuation approaches and standards for crypto-assets have been recently developed. Besides, there are discussions within the international valuation organisations to include digital assets in their scope; European Financial Reporting Advisory Group (EFRAG), Accounting for Crypto-Assets (Liabilities): Holder and Issuer Perspective (July 2020); Chartered Business Valuators (CBV) Institute, Decrypting Crypto: An Introduction to Cryptoassets and a Study of Select Valuation Approaches (2019); PWC, In depth A look at current financial reporting issues, Cryptographic assets and related transactions: accounting considerations under IFRS (No. 2019-05, December 2019).

Annex III – Appendix 3 – SUB-GROUP 3 – Secured transactions

Sub-Appendix A – Digital Assets and Security Rights – Special Sections

"Digital twins" and commercial paper

1. The notion of a digital asset embodying, representing or being linked to a real-world asset ("digital twins") is comparable to the concept of a "commercial paper" (*Wertpapier* in German), variants of which are known in most legal systems. This sub-section uses the term "embodies" as a synonym for "represent" and "link" when the consequence under the applicable law is for the document/record to convey rights to the underlying goods. This is opposite to "evidences" where the consequence under the applicable is for the document/record merely to describe some quality of the goods, but its transfer does not convey any rights to the goods (e.g., a certificate of quality). Generally speaking, a commercial paper embodies a right in such a manner that holding the document is equated to holding the right; the two cannot be separated. For example, the right can only be exercised, enforced, or transferred by the holder of the document. Many examples of such documents exist, such as bills of exchange, promissory notes, cheques, share certificates and other securities. Although commercial papers, as physical documents, are objects of property themselves, their main characteristic is that they embody other rights, such as personal rights (the right to receive payment) or other intangible assets (a right to participate in an enterprise). Some commercial papers also embody rights to tangible goods, including possession or title (ownership). The former situation (embodying legal possession) essentially entails the right to demand delivery of tangible goods from a person who has been entrusted with physical possession of the goods. Such documents that embody title or right to possession of physical goods are often referred to as "documents of title" (*Traditionspapier* in German) or negotiable documents (the UNCITRAL Model Law on Secured Transactions). The most common examples globally are bills of lading, warehouse receipts and functionally equivalent documents. In other words, documents of title typically operate in the context of goods being deposited with a person for storage or transportation purposes.

2. Many legal systems have, through legislation, rendered commercial papers (especially bills of exchange) negotiable in order to protect good faith acquirers of the document. [cross-reference to SG2 Principles on "innocent acquisition]. However, this is not always the case with documents of title where the applicable law may provide more or less protection to acquirers against pre-existing claims (compare Articles 46 and 49 of the UNCITRAL Model Law). The exact legal nature of a document of title and its relationship to the underlying asset is a complicated matter because, unlike documents embodying personal rights, documents of title purport to have a proprietary effect, which is conceptualised differently in legal systems. For example, in the United States, in the case of a negotiable document of title (bills of lading and warehouse receipts), Article 7-502 of the Uniform Commercial Code (UCC) provides that the due negotiation of the document has the legal effect that the holder receives title to the goods. In English law, on the other hand, a bill of lading grants the right to demand possession (delivery) from the person in physical possession of the goods, and this right to demand possession can be transferred by transferring the document.[29] However, the right to demand delivery will only be transferred in this case if the transferee of the document also has a proprietary right, like ownership, or a contractual right (e.g. under a contract of carriage) to claim delivery.[30] This approach is followed in, for example, South

[29] See e.g.., *Heskell v Continental Express Ltd* 1950 1 All ER 1033 at 1042.

[30] See e.g.., *The "Future Express"* 1992 2 Lloyd's Rep 79 at 96.

Africa[31] and Australia[32] as well. Another way to put it is that, under both English and South African law (and the same appears to be true under German and Dutch law), the document places its holder in "symbolic" possession of the goods, and transfer of the document amounts to symbolic transfer of possession of the goods. Under all of these laws, the document can be transferred to a creditor to create a security right in the underlying goods to, placing the latter in legal possession of the goods – the document being the symbol of possession.

3. The UN *Convention of Contracts for the International Carriage of Goods Wholly or Partly by Sea* (the "Rotterdam Rules"), which is not yet in force, uses the concept of the "right of control" and refers to the holder of the transport document (i.e. bill of lading) as the "controlling party".[33] The "right of control" is defined as "the right under the contract of carriage to give the carrier instructions in respect of the goods",[34] while "controlling party" is defined as "the person that … is entitled to exercise the right of control".[35] The right of control can only be exercised by giving or modifying instructions to the carrier, obtaining delivery of the goods, or replacing the consignee.[36] The controlling party also has the right to transfer the right of control to another person by transferring the transport document or electronic transport record to that person.[37] Chapter 3 read with Chapter 8 of the "Rotterdam Rules" allows for the recording of anything contained in a transport document (i.e. bill of lading) in an electronic transport record. The issuance and transfer of control of this electronic transfer record will then have the same effect as that of delivery of a "paper" transport document.

4. There are two ways in which a document can become a document of title, which may provide the basis for conceptualising a digital asset as a "digital asset of title" (digital twin / tethered asset). The first is through statutory recognition. Codified civil law systems usually take this approach, examples being Germany[38] and the Netherlands.[39] Even in such cases, the legislative recognition was usually preceded by mercantile practice and other developments.[40] Statutory recognition can also be employed to recognise documents of title

[31] See e.g.., *London and South African Bank v Donald Currie & Co* (1875) 5 Buch 29 at 33-34; *Lendalease Finance (Pty) Ltd v Corporacion De Merçadeo Agricola and Others* 1976 (4) SA 464 (A) at 492. See further SF Du Toit 'The evolution of the bill of lading' (2005) 11 *Fundamina* 12-25; SF Du Toit 'The legal nature of silo receipts used in the futures market and bills of lading' 2007 *TSAR* 56-71; SF Du Toit 'Silo Receipts used in the futures market and bills of lading as documents of title (part 1)' 2007 *TSAR* 223-239; SF Du Toit 'Silo Receipts used in the futures market and bills of lading as documents of title (part 2)' 2007 *TSAR* 452-468.

[32] R Ashton 'A comparison of the legal regulation of carriage of goods by sea under bills of lading in Australia and Germany' (1999) 14(II) *Aust & NZ Mar LJ* 24-64 at 26.

[33] Chapter 10. See G van der Ziel 'Chapter 10 of the Rotterdam Rules: Control of goods in transit' (2009) 44(3) *Texas Intl LJ* 375-386.

[34] Article 1(12) of the Rotterdam Rules.

[35] Article 1(13) of the Rotterdam Rules.

[36] Article 50(1) of the Rotterdam Rules.

[37] Article 51(2)(a), (3)(a) and (4)(b) of the Rotterdam Rules. The Rotterdam Rules also makes it possible to be a controlling party and exercise the right of control without the presence of any documents, and in this case, the transfer of the right of control will be effective against the carrier via notification to the latter; see Article 51(1).

[38] The three documents of title (*Traditionspapiere*) recognised by the German Commercial Code (*Handelsgesetzbuch*) are the inland waterway bill of lading (*Ladeschein* - §443), the bill of lading (*Konnossement* - §515) and the warehouse warrant/receipt (*Lagerschein* - §475). See also §363.

[39] The Dutch Civil Code (*Burgerlijk Wetboek*) recognises four documents of title: the combined transport (*gecombineerd vervoer*) document (*CT-document* - Book 8 Article 50); the inland water transport (*binnevaart*) bill of lading (*cognossement* - Book 8 Article 924); the ocean transport (*zeevervoer*) bill of lading (*cognossement* - Book 8 Article 417); and the custodian (*bewaarnemer*) document (*ceel* - Book 7 Article 607).

[40] See AJ Van der Lely 'Levering door middle van een ceel: Enige opmerkingen over een zakenrechtelijk waardepapier in het Nederlandse recht vanaf 1815' (1993) 10 *Groninger Opmerkingen en Mededelingen* 94-118 for an interesting discussion on the historical development of a *ceel* as document of title in the Netherlands.

in digital format.[41] This is presently the case with respect to the implementation of the UNCITRAL Model Law on Electronic Transferable Records.

5. The first method may also invite courts to recognise certain records as documents of title through a broad statutory definition. For instance, UCC 1-201 defines a document of title as "…also any other document which in the regular course of business or financing is treated as adequately evidencing that the person in possession of it is entitled to receive, hold, and dispose of the document and the goods it covers."

6. The second method, which is best illustrated by English law, is where a document is recognised by the courts as a document of title, without any statutory definition, – typically because participants in that market have, over many years, come to treat the documents in that way. Simply put, the courts in England have given legal recognition to an established mercantile practice or custom in this regard.[42] However, that has not been the case for other documents, which generally are treated as documents of title in other jurisdictions, particularly warehouse receipts. The courts relied, amongst others, on the fact that there was a clear practice and that it was universally recognised by merchants that bills of lading represent possession of goods.[43] This way of dealing with physical goods transported by sea developed for the sake of convenience.[44] Importantly, the terms of the document are not enough to make it a document of title; this can only happen via mercantile custom or statute.[45]

7. It may be possible for a commercial practice to develop whereby a digital asset is regarded as something akin to a "document of title" in a particular context and for the courts to recognise the same. However, in jurisdictions where this could happen (like England), it would require an established mercantile custom that is universally recognized by participants in that industry. Presently, this might be an insurmountable hurdle with digital twins, since the latter practice is very new when compared to the many decades of mercantile practice that preceded the recognition of bills of lading as documents of title by the courts. Furthermore, in the rapidly changing environment – with new products appearing on the market almost on a weekly basis – it is likely impossible to identify a universally accepted custom of certain digital tokens representing title, or other property rights such as possession of certain tangible goods. For all intents and purposes, bills of lading (and similar documents) are almost the only way in which goods are transferred during sea transport. However, the same cannot be said for, for instance, the ownership/possession of gold via digital tokens. In other words, mercantile custom cannot realistically be relied upon as a way for digital tokens to become recognised as documents of title.[46] Therefore, the more feasible approach is to develop legislation that clearly sets out the conditions under which a digital asset can legally represent either the right to demand delivery or ownership of a tangible good.[47]

[41] See §§443(III), 475(c) and 516(II) of the *Handelsgesetzbuch*. See also D Saive 'Blockchain documents of title – Negotiable electronic bills of lading under German law' (23 Jan 2019), available at https://ssrn.com/abstract=3321368 (accessed 2 Jun 2021).

[42] *Lickbarrow v Mason* (1793) 2 H Bl 211 (126 ER 511); (1794) 5 TR 683 (101 ER 380); *Barber v Meyerstein* (1870) LR 4 HL 317; etc.

[43] See e.g.., *Sanders Brothers v MacLean & Co* (1883) 11 QBD 327 at 341.

[44] *Barber v Meyerstein* (1870) LR 4 HL 317 at 329-320.

[45] *The "Future Express"* 1992 2 Lloyd's Rep 79 at 95.

[46] The only exception could be where a bill of lading or other established document of title is digitized so that the digital token takes the place of the physical document, but even this would likely require legislative intervention.

[47] Although, as in the case of German law or the Rotterdam Rules, there might be other jurisdictions who also already accommodate digitized documents of title, which may or may not be broad enough to allow for tokenization.

8. When a digital twin springs up the secured transaction law should be flexible enough to enable its transfer to a secured creditor for the purpose of securing an obligation. A secured transactions law, based on the UNCITRAL Model Law, would apply to any digital twin, but would not determine whether a security right in the digital asset also conveys a security right in the tangible asset it purports to embody. A secured transactions law may need to be coordinated with the underlying law that governs which assets constitute "digital twins". It has been forward-looking with respect to not only recognising various types of documents of title in the statute itself, but also supporting development of customs that may generate "digital twins".

9. The secured transactions law should thus consider including a definition of a digital twin, analogous to the definition of negotiable document, along the lines of "*a record, such as* [enacting State to insert references to records that are already treated in the market as 'digital twins'] *that embodies a* [title, right to delivery of tangible assets, or other property right consistent with the law governing documents of title] *and satisfies the requirements for negotiability*."

10. The asset-specific rules for the creation, third-party effectiveness (control) and enforcement of security rights may be the same as for electronic negotiable documents. However, the priority rules may need to be different as negotiable documents present issues specific to the financing practices to the industry. For instance, the priority of a secured creditor may vary based on whether the negotiable document covers goods held as inventory or equipment, as reflected in paragraphs (1) and (2) of Article 49 of the UNCITRAL Model Law, respectively.

11. The relevant conflict of law rule may need to be crafted for security rights in digital twins. According to Article 85(2) of the UNCITRAL Model Law, the priority of the security right in the case where the security right had been perfected by possession of the document will be the law of the State in which the document is located; not the law of the State where the asset is located. The reasoning behind this is that the law applicable to the document would better reflect the legitimate expectations of the parties, while the outcome would also be more consistent with the substantive rules regarding the creation, third-party effectiveness and priority of security rights in negotiable documents.[48] This conflict of laws approach would need to be adapted to cases where the tangible asset is represented by a digital asset – mostly because a digital asset does not have a physical location.

[48] UNICITRAL Legislative Guide on Secured Transactions Ch 10 para 27 at p. 389.

Prevailing DeFi practices and features

Introduction

12. "DeFi" refers to Decentralized Finance, which combines various technologies that collectively provide decentralized or disintermediated means of executing traditional financial transactions using crypto assets.[49] DeFi is based on blockchain and open-source software, and therefore is generally open and available to be used by any person with compatible technology and assets without relying on traditional centralized financial intermediaries such as brokerages, exchanges, or banks. DeFi systems may involves transactions with various types of digital assets, including cryptocurrencies, stablecoins and tokens. In these transactions, digital assets may be used as collateral for various obligations. For instance, a DeFi user may either "borrow" funds by granting "security" over a digital asset or "loan" out the digital asset in return for a form of financial compensation – either a return paid in a digital asset or a new digital asset.

13. During the previous session, the Working Group asked SG3 to provide some background on how the transactional structures, particularly those used in DeFi systems may be affected by secured transactions laws. The Working Group may wish to specifically assess the type of interest granted over digital assets in DeFi systems and examine whether such transactions fall within the traditional concept of secured transactions and, accordingly, whether and how the relevant law applies.

14. DeFi services are offered by DeFi providers, which may or may not be entities constituted under some law, such as companies. DeFi providers offer their services in the form of software accessible through webpages or apps, thus performing decentralized financial functions similar to those of traditional finance providers. In other words, DeFi providers offer decentralized versions of financial services, making financial products available on a public blockchain network without traditional intermediaries. The term "DeFi providers" may be used as an umbrella term focusing on service provision, similar to the use of the term traditional finance providers, without specific focus on the actors who offer the services. The terms "applications" and "platforms" are used interchangeably to refer to the services provided by those providers. In practice, a DeFi provider offers a distributed application (Dapp) that may be used by others. Most DeFi providers describe themselves as software providers rather than financial intermediaries. Providers and applications are part of the decentralized ecosystem, through which the users interact with each other on a peer-to-peer basis. "Protocols", on the other hand, refer to specific DeFi providers which run on smart contracts and are, therefore, based on an automatic set of rules.

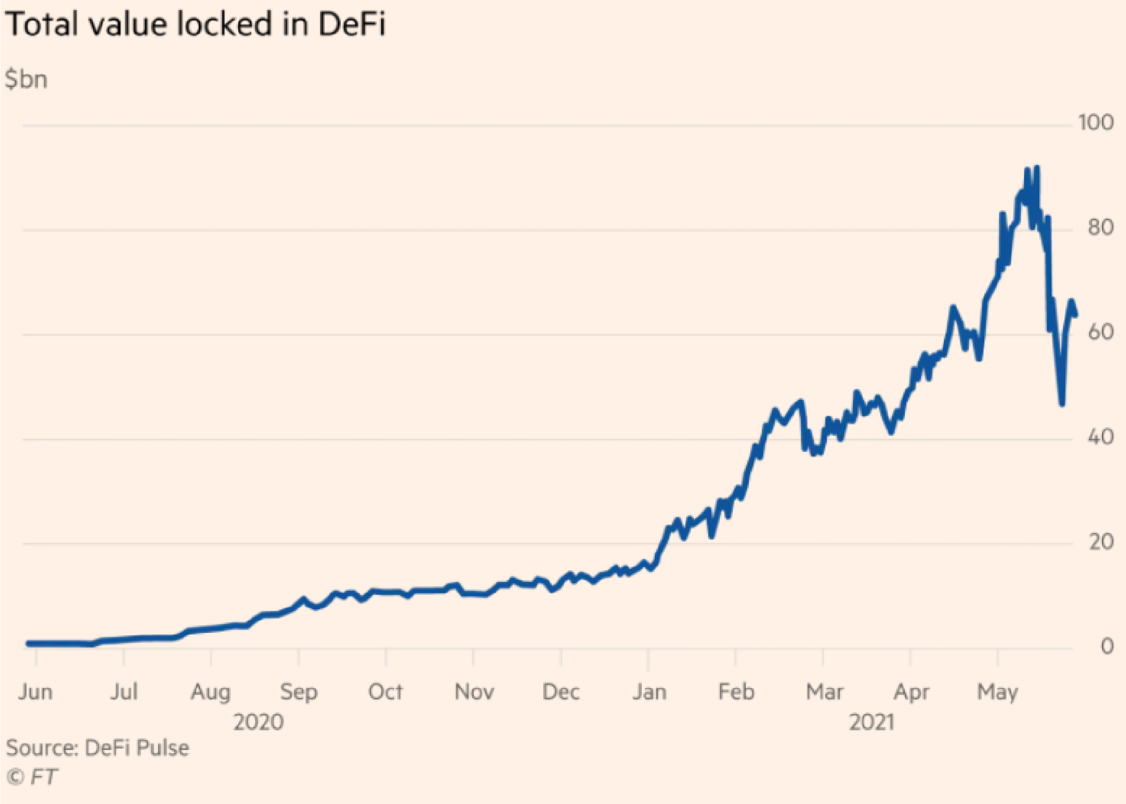
- The Working Group may wish to consider some of these terms, such as "applications" and "platforms" for the taxonomy purposes of the Project.

15. DeFi providers often use similar structures but may differ on fees, interest rates and types of supported digital assets. Some provide more transparent policies and practices through clearer terms of use. In addition, some DeFi providers, especially those in the form of protocols, use native tokens which may represent a user's share of the overall amount of deposits held in aggregated buckets of assets known as "liquidity pools" (see below in Trading services). Each of these tokens represents the balance of digital assets provided by a given user. Native tokens may often accrue interest in real time while the underlying asset is loaned out or otherwise used by others in a manner designed to provide an economic return. Other native tokens allow users to participate in the governance structure of the DeFi protocol.

[49] "Broadly, it is a category of blockchain-based decentralized applications (DApps) for financial services": http://www3.weforum.org/docs/WEF_DeFi_Policy_Maker_Toolkit_2021.pdf.

16. DeFi systems are not generally insured, which leaves their users exposed to high risks. For instance, in case the user's assets are lost, including in a fraudulent transaction, the user may have no recourse against any identifiable person, and if a person may be identified, the user may have an unsecured claim.

17. The DeFi sector is growing and the value of digital assets therein is rapidly increasing. According to data from DeFi Pulse and FT[50], the value of cryptocurrency being used as collateral for loans and other transactions with DeFi providers has recently reached the amount of $67bn. Similarly, the total value locked in DeFi, reflecting the amount of underlying supply being secured by DeFi providers, has significantly grown in 2021, hitting approximately $90bn while in 2020 it topped around $15bn:


Total value locked in DeFi

Source: DeFi Pulse
© *FT*

Description of DeFi services

18. In particular, DeFi providers offer the following services:

"Depositing" services

19. DeFi users can transact (i.e., "deposit") digital assets in return for compensation in the form of other or additional digital assets. In practice, this occurs by transferring control of a digital asset from the user's personal wallet to the account or wallet they obtain in the DeFi provider's system. By transferring control of those assets, users (i.e., "depositors") generally are required to affirm (via a click-wrap type agreement) that they own them. By transferring control of a digital asset users can i) earn interest (Depositing services), ii) trade the digital assets, often while accruing interest (see Trading services) iii) offer the assets as collateral to borrow other digital assets or funds (sometimes denominated in fiat currency), although usually without earning interest at the same time (*see* Lending services). The terminology

[50] "Silicon Valley bets on crypto projects to disrupt finance" (Financial Times, 03.06.2021).

used by the providers of the depositing services includes "depositing", "holding", "transferring", "pledging" and "renting" of digital asset. The wording, as well as the mechanism by which digital assets are transferred to the DeFi provider, create doubts on the actual nature of the transactions and, especially, on the type of interest the depositor retains in the digital asset.

20. After users transfer their assets, the DeFi provider (i.e., recipient) takes control of them by "locking them up" in the smart contract, in exchange for a payment at a variable interest rate executed by the code. Most DeFi systems offer rates of return on digital assets which are much higher than those available through traditional, regulated depository institutions. This interest derives from yield-producing activities conducted by the DeFi providers, including offering loans to third parties (*see Lending services*) or using the assets provided by their users in other yielding structures. DeFi providers often use the deposited digital assets as collateral to access credit from third parties (i.e., they rehypothecate the digital asset). The wording of several DeFi terms of use (see below) and market reports demonstrate that rehypothecation is an established industry practice.

21. The description of the depositing services indicates the presence of at least three parties: i) the initial depositor who transfers digital assets to the DeFi provider, ii) the recipient, i.e., DeFi provider; and iii) the DeFi provider's creditor, i.e., someone that provides credit to the DeFi provider against the security of digital assets (rehypothecation).

Lending services

22. DeFi providers offer loans to third parties (usually to institutional and corporate borrowers) against digital assets. Generally, two types of "crypto-backed loans" are provided:

(a) Lending of digital assets to third parties. DeFi providers lend the digital assets that users deposit under the "depositing services".

(b) Lending of funds (US dollars or stablecoins) to third parties. Often, the funds are generated from a conversion of the digital assets deposited under the depositing services. Many DeFi providers convert the digital asset on deposit to US dollars, and then lend the funds to third parties.

23. Users provide their digital assets as collateral following the procedure of the depositing services above. The loans must be repaid with interest. The interest generated is partially given by the DeFi providers to the users depositing the digital assets (*see* Depositing services), while the rest is retained by the DeFi provider as profit. The profit portion of the interest is then frequently distributed to "governance token holders" as discussed below in Trading services. In fact, DeFi providers use deposits to attempt to obtain higher yields than those which they offer to their users. Depending on the DeFi provider's policy, some digital assets offered as collateral for loans can, in the meantime, generate interest for their user, in accordance with the depositing services described above.

24. To ensure loan performance and reduce the risk of high volatility inherent in many digital assets, lending services are usually provided on overcollateralized terms. This means that DeFi providers loan up to a specific amount of the value of collateral (usually up to 50-70%). DeFi providers impose specific collateral thresholds and requirements to prevent liquidation of the collateral and the closure of the position. The ratio of credit or borrowed asset to the value of the deposited asset is crucial in this regard. If the collateral ratio reaches a pre-determined limit and falls below the minimum threshold, the collateral of the depositor can be liquidated. This means that the collateral provided by the depositor is sold but that the depositor keeps the amount borrowed. To prevent liquidation, some systems issue the equivalent of a margin call which allows the user to deposit more collateral or repay the loan. If the collateral ratio increases following a rise of the collateral value, the system grants the

user a power to withdraw additional funds, respecting the collateralization ratio minimums. In practice though, users do not exercise this power.

Trading services

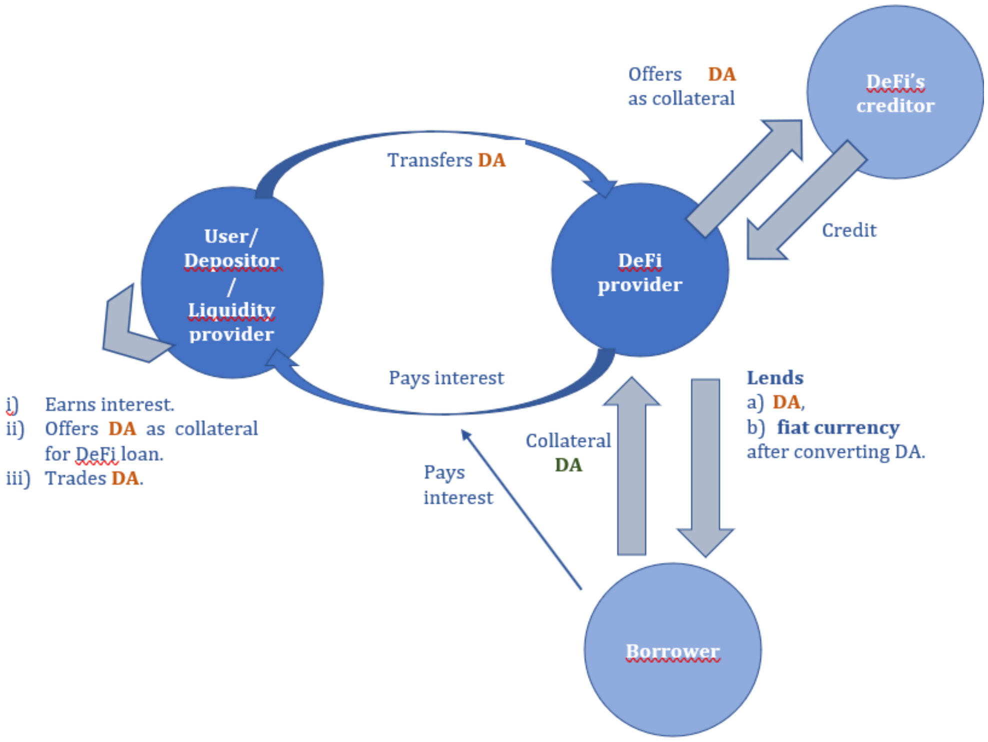
25. DeFi users can buy, sell or exchange one digital asset class for another (e.g., Bitcoin <-> Ether). Rather than using a centralized order book and market-makers, certain DeFi systems offer trading through a "liquidity pool", which is a smart contract also known as an Automatic Market Maker (AMM). The depositors contribute pairs of digital assets to the "liquidity pool" or "LP" and become liquidity providers. Essentially, LPs constitute a collection of funds locked in a smart contract and powering a marketplace for decentralized financial operations.

26. Each LP holds a pair of assets; the ratio of asset to asset becomes the "price" for a trader. For example, if a pool holds 5,000 x coin and 500 y coin, the trading price at that time would be 10 x coin to 1 y coin. If a user wishes to provide additional liquidity, they would be required to contribute both x coin and y coin at the same ratio: 10 x coin to 1 y coin. In exchange for providing liquidity into a pool, the liquidity providing user obtains a liquidity pool ("LP") token which provides it with a claim to a proportionate share of the overall liquidity of both x and y coin, and which can be used as collateral or to otherwise interact with other DeFi systems. Many DeFi providers offer interest accrual (on the LP token) to users of trading services.

27. If a trader wanted to purchase 100 y coin from the LP, they would be required to pay 1000 x coin. That transaction would result in the new balance of assets in the LP indicating 6000 x coin and 400 y coin adjusting the transaction price to 15 x coin to 1 y coin. When a given LP contains a high level of assets, individual transactions have less impact on an asset's trading price in a given LP. Thus, liquidity pools permit users to exchange one digital asset for another while maintaining a balance via a progressively priced balancing algorithm which adjusts the exchange rate.

28. LPs create an opportunity for arbitrage since the new exchange rate is out of balance with the exchange rate available elsewhere. LPs assume that arbitrageurs will trade in the direction opposite to a given acquirer's transaction if that transaction results in a material deviation between prices for a given asset in an LP versus those in other markets, eventually bringing the LP exchange rate for a given asset pair on the LP closer to market exchange rates elsewhere.

DeFi digital assets flows:



Examples of DeFi Terms of Use

29. Below is a selection of terms used by a variety of DeFi providers:

Example 1

Interest Account Terms

Consent to Utilize Assets

1. Except where prohibited or limited by applicable law, in consideration for the cryptocurrency earned on your account, you grant [us] the right, without further notice to you, to hold the cryptocurrency held in your account in [our] name or in another name, and to pledge, repledge, hypothecate, rehypothecate, sell, lend, or otherwise transfer, invest or use any amount of such cryptocurrency, separately or together with other property, with all attendant rights of ownership, and for any period of time and without retaining in [our] possession and/or control a like amount of cryptocurrency, and to use or invest such cryptocurrency at its own risk.

2. You acknowledge that, with respect to assets used by [us] pursuant to this paragraph: (i) you may not be able to exercise certain rights of ownership, (ii) [we] may receive compensation in connection with lending or otherwise using or investing cryptocurrency in its business to which you will have no entitlement, and (iii) cryptocurrency that is subject to such lending transactions, investment or otherwise being used in these transactions will not be held by [our] third party custodians.

Setoff and Security Interest Rights

3. You grant us a security interest in any and all of your Crypto Interest Accounts with us for obligations owing to us or any of our affiliates by any owner of any of your accounts. These obligations include both secured and unsecured debts and debts you owe individually or

together with someone else, including debts and obligations under other transactions or agreements between you and us or any of our affiliates.

4. We may take or set off funds in any or all of your Crypto Interest Accounts, or transfer funds between any of all of your Crypto Interest Accounts, with us or any of our affiliates for direct, indirect and acquired obligations that you owe us or our affiliates, including any balances as a result of not having sufficient funds available or as a result of an erroneous transfer of funds to an address under your control, or a return or other negative balance, regardless of the source of funds in an account.

<u>Example 2</u>

Terms of Use

Setoff and Security Interest Rights

1. Your acceptance of these Terms serves as your consent to [us] asserting its security interest or exercising its right of setoff should any laws governing your […] Wallet require your consent.

Risk Disclosure

2. These Terms and the holding of Digital Asset relationship does not create a fiduciary relationship between us and you; your […] Wallet is not a checking or savings account, and it is not covered by insurance against losses. We may lend, sell, pledge, hypothecate, assign, invest, use, commingle or otherwise dispose of assets and Eligible Digital Assets to counterparties or hold the Eligible Digital Assets with counterparties, and we will use our best commercial and operational efforts to prevent losses.

3. Eligible digital assets in your […] wallet are not held by [us] as a custodian or fiduciary, are not insured by any private or governmental insurance plan (including the federal deposit insurance corporation (FDIC) or the securities investor protection corporation (SIPC)), and are not covered by any compensation scheme (including the financial ombudsman and financial services compensation scheme (FSCS)).

Consent to [Our] Use of Your Digital Assets

4. In consideration for the rewards earned on your […] Wallet and the use of our Services, you grant [us], subject to applicable law and for the duration of the period during which the Digital Assets are available through your […] Wallet, all right and title to such Digital Assets, including ownership rights, and the right, without further notice to you, to hold such Digital Assets in [our] own virtual wallet or elsewhere, and to pledge, re-pledge, hypothecate, rehypothecate, sell, lend, or otherwise transfer or use any amount of such Digital Assets, separately or together with other property, with all attendant rights of ownership, and for any period of time, and without retaining in [our] possession and/or control a like amount of Digital Assets or any other monies or assets, and to use or invest such Digital Assets. You acknowledge that with respect to Digital Assets used by [us] pursuant to this paragraph:

> (i) You may not be able to exercise certain rights of ownership; (ii) [we] may receive compensation in connection with lending or otherwise using Digital Assets in its business to which you have no claim or entitlement; (iv) [we] may use your Eligible Digital Assets as collateral to borrow other digital or fiat assets in different jurisdictions around the world. While such borrowing are for the purpose of optimizing the returns to all members, [we] may experience losses or partial recovery of such collateral in certain situations; and (v) [we] may lend your coins to exchanges, hedge and other counterparties, which may provide full or partial collateral for any coin or fiat loan.

Legal Process Affecting […] Wallets

5. Any garnishment or levy against your […] Wallet is subject to our right of setoff and security interest.

<u>Example 3</u>

Terms of Use

Digital Currency Title

All Digital Currencies held in your Digital Currency Wallet are assets held by the […] Group for your benefit on a custodial basis. Among other things, this means:

> (A) Title to Digital Currency shall at all times remain with you and shall not transfer to any company in the […] Group. As the owner of Digital Currency in your Digital Currency Wallet, you shall bear all risk of loss of such Digital Currency…
>
> (B) None of the Digital Currencies in your Digital Currency Wallet are the property of, or shall or may be loaned to, […]; […] does not represent or treat assets in a user's Digital Currency Wallets as belonging to […]. [We] may not grant a security interest in the Digital Currency held in your Digital Currency Wallet…

<u>Example 4</u>

Terms of Use

Custody of Cryptocurrency

1. [We are] a custodian of any Cryptocurrency transferred to […] Accounts. [We do] not obtain any legal or beneficial right, title or interest in your Cryptocurrency stored in your Account.

Legal Process Affecting Accounts

2. Any garnishment or other levy against your account is subject to our right of setoff and security interest.

Setoff and Security Interest Rights

3. You grant us a security interest in any and all of your accounts with us for obligations owing to us or any of our affiliates by any owner of any of your accounts. These obligations include both secured and unsecured debts and debts you owe individually or together with someone else, including debts and obligations under other transactions or agreements between you and us or any of our affiliates. We may take or set off funds in any or all of your accounts, or transfer funds between any of all of your accounts, with us or any of our affiliates for direct, indirect and acquired obligations that you owe us or our affiliates, including any balances as a result of not having sufficient funds available or as a result of an erroneous transfer of funds to an address under your control, regardless of the source of funds in an account.

4. We may consider these Terms as your consent to [our] asserting its security interest or exercising its right of setoff should any laws governing your account require your consent.

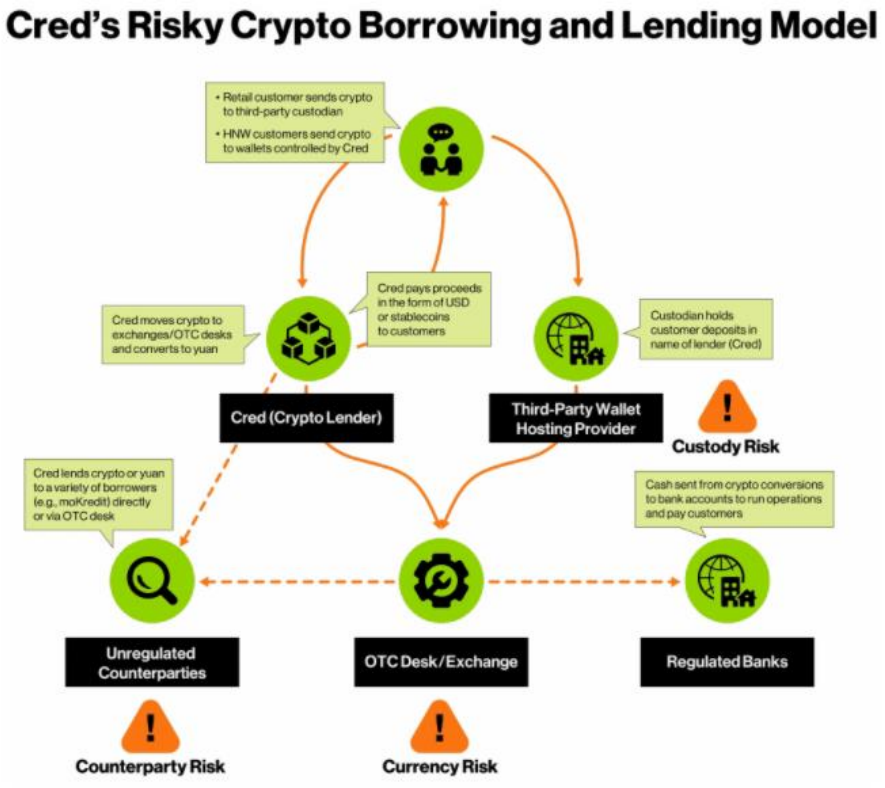
Cred bankruptcy case

The case regards Cred Inc., a centralized cryptocurrency lender that filed for bankruptcy in November 2020 (US Bankruptcy Court for the District of Delaware). Cred is a cryptocurrency investment platform, describing itself as a "global financial services platform" and "licensed lender" that delivers lending and borrowing services to customers in 183 countries.

Cred's primary financial product, "Cred Earn," enables customers to earn interest (10%) on their cryptocurrency holdings pursuant to a sort of a lending contract. In practice, retail customers transfer their crypto either directly to Cred or to third party e-wallets via the Cred portal in order to receive a monthly interest by Cred paid in crypto, stablecoins or fiat (dollars). Cred lends its customer's crypto to third parties including asset managers and crypto mining companies (CredBorrow product). One of them is moKredit, a Chinese lending service. Cred used to convert depositors' cryptocurrency to yuan and then lent those funds to moKredit, which, in turn was using them to provide small lines of credit in the form of digital tokens. In other words, Cred lent customer crypto to moKredit to finance its own micro-lending activities. Eventually moKredit became highly leveraged and could not repay Cred nor provide the expected annual interest.

A combination of specific financial situations led to Cred's collapse. As customer deposits, in the form of cryptocurrency like Bitcoin, are a liability on Cred's balance sheet, the latter was negatively impacted following a recent rise of BTC's price and led to high liquidity risk. As Cred was investing the deposited crypto with third parties, Cred did not itself hold significant amounts of crypto and had to purchase new crypto at the then prevailing prices every time it had to repay customers. In addition, Cred suffered a hack and had to freeze customer cryptocurrency funds. Besides, the firm was allegedly accused of failing to comply with corporate responsibility rules and to prevent fraud and loss of funds.

Cred's money flows:



Cred's Risky Crypto Borrowing and Lending Model

- Retail customer sends crypto to third-party custodian
- HNW customers send crypto to wallets controlled by Cred

Cred moves crypto to exchanges/OTC desks and converts to yuan

Cred pays proceeds in the form of USD or stablecoins to customers

Custodian holds customer deposits in name of lender (Cred)

Cred lends crypto or yuan to a variety of borrowers (e.g., moKredit) directly or via OTC desk

Cash sent from crypto conversions to bank accounts to run operations and pay customers

Slide from Paul Hastings presentation in bankruptcy hearing. *(U.S. Bankruptcy Court, Delaware)*

Other takeaways:

- According to Cred's website, Cred offers 2 types of services: 1) "hold with interest" (Rental agreement)[51], 2) Pledge agreement.[52]
- According to Cred's website, "The pledged assets are used to lend to customers…". But the mechanics of the transaction do not suggest a classic pledge occurs; rather the digital asset is "rented" or transferred similarly to a securities repo.
- According to Cred's Liquidation Plan of 21.01.2021: "The Debtors have not issued any secured debt. In August and September 2020, Cred issued the Convertible Notes."[53] Of Cred's $136 million in liabilities, $114 million is owed to holders of Cred Earn notes.[54] According to Coindesk, Cred launched the earnings product 'Cred Earn', after the markets crashed in December 2018. The product seemed to be similar, at least superficially, to a certificate of deposit at a bank. "The new product's users signed unsecured notes to Cred, closer to lending money to a company than depositing it in an FDIC-insured bank, one employee said. (According to insiders, in the first quarter of this year the company's capital markets team proposed a liquidation plan that would have prioritized repayment to Cred Earn noteholders over other creditors in the event of failure…".[55]

[51] Shortly before the Petition Date, the Debtors began using contracts to "rent" Cryptocurrency from Customers. As of the Petition Date, rental contracts accounted for less than 1% of the Debtors' Customer contracts; p. 14 of the Liquidation Plan (21.01.2021) https://dr201.s3.amazonaws.com/cred/Plan%20and%20Disclosure%20Statement.pdf

[52] See https://mycred.io/earn/

"Cred (US) LLC is a licensed lender and allows some borrowers to earn a yield on cryptocurrency pledged as collateral. Cred (US) LLC also rents cryptocurrency from users and pays rental fees calculated as an interest rate yield. The yield feature, whether as part of a pledge or a rental agreement, is sometimes referred to as CredEarn."

[53] p. 15 of the Liquidation Plan (21.01.2021).

[54] This was stated by Cred's former head of capital markets, Daniyal Inamullah.

https://www.coindesk.com/bad-loans-bad-bets-bad-blood-how-crypto-lender-cred-really-went-bankrupt.

[55] See Nate DiCamillo, *Bad Loans, Bad Bets, Bad Blood: How Crypto Lender Cred Really Went Bankrup,* (Coindesk) November 2020 at https://www.coindesk.com/bad-loans-bad-bets-bad-blood-how-crypto-lender-cred-really-went-bankrupt.

Appendix 4 – SUB-GROUP 4 – Taxonomy & PIL

Taxonomy

1. This note provides an update on the taxonomy work stream and reflects discussions at the Second and Third Sessions,[56] the 'Digital Twins' Workshop,[57] and the outcome of the information-gathering exercise launched within the Taxonomy and Private International Law Sub-Group on 23 September 2021.[58]

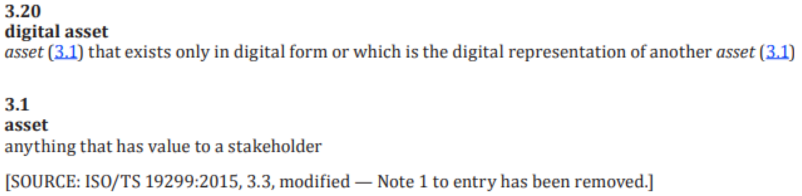
Approach to the definition of 'digital asset'

2. Having previously discarded functional approaches (typically applied in regulatory settings[59]) as unsuitable, having previously agreed that 'digital asset' should be constitutive of something rather than being simply evidentiary,[60] and following a re-iteration of the need for a wide scope definition (with the possibility of exclusions in due course e.g. gaming tokens), at the Third Session a working definition of 'digital asset' emerged as follows:

> *'**Digital asset**'*
> *A digital asset is an **electronic record** which **gives rights to** the holder is **capable of being subject to control**.*

3. Put simply, it was agreed that the term is narrower than 'electronic record' – hence the importance of the words 'capable of being subject to control'. However, Project members continued to express a range of views on the need to represent the notion of 'rights' and/or also the notion of 'value'.

4. On the latter point ('value'), and in view of the strong desire of Project members to avoid definitions used in regulatory context and to avoid favouring approaches used in specific jurisdictions, it is identified for interest that ISO 22739 (first edition 2020-07) (Blockchain and distributed ledger technologies – Vocabulary) defines 'digital assets' as follows:



3.20
digital asset
asset (3.1) that exists only in digital form or which is the digital representation of another *asset* (3.1)

3.1
asset
anything that has value to a stakeholder

[SOURCE: ISO/TS 19299:2015, 3.3, modified — Note 1 to entry has been removed.]

5. On the former point ('right'), it is noted that for reporting purposes some companies/institutions in some jurisdictions have started to rely on the following definitions:

[56] Second Session 16 -18 March 2021; Third Session 31 June - 2 July 2021.

[57] 31 May 2021.

[58] The template was issued to Sub-Group members in Excel format with an initial response deadline of 7 October, the deadline was extended to 15 October 2021.

[59] For example: (i) exchange tokens, (ii) security/investment tokens, (iii) utility tokens, and (iv) hybrids.

[60] Second session.

> ***'Digital asset'***
>
> *A digital asset is an electronic record in which an individual has a right or interest. They do not exist in physical form. The electronic record is the asset.*
>
> ***'Digitised asset'***
>
> *A digitised asset is an asset (which may be a security or physical asset) the ownership of which is represented in an electronic record (e.g. ownership of real estate represented on a digital ledger). It is an electronic record of ownership of the asset.*
>
> *Digital and digitised assets are represented on an electronic ledger that is not necessarily a blockchain. The process of digitising assets is also referred to as "tokenisation".*
>
> [i.e. whether the digital token *is the asset* or *evidence of a claim in respect of* an asset]

6. Overall, it was agreed that the approach to the definition of 'digital asset' will be necessarily iterative in line with evolutions in the Project's work.

Categories of 'digital asset'

7. As discussed at the Second and Third Sessions **two basic categories of 'digital asset**' can be identified (essentially leveraging the 'native' vs 'non-native' categorisation with an aim to avoid the terms as there is a general recognition these terms have a particular use by technicians in the sphere of digital-asset development):

- Category 1: digital asset constituting [a claim] in respect of:[61]
  (i) a moveable tangible
  (ii) an immoveable tangible
  (iii) a tokenised currency, of which two fundamentally distinct categories:
    - privately tokenised fiat funds (e.g. the utility settlement coin[62])
    - central bank digital currency (CBDC)
  (iv) an intangible financial asset
  (v) an intangible non-financial asset (e.g. IP)

- Category 2: digital asset that is not a Category 1 asset*.*

8. At the Second and Third Sessions it was agreed that, for the purposes of the Project's work, the distinction between Category 1 and 2 is highly relevant (i.e. between 'native' and 'non-native'/ 'endogenous' and 'exogenous').

[61] Category 1 is sub-categorised by reference to the type of asset to which the claim relates.
[62] https://www.fnality.org/home

9. It was also agreed at the Third Session that, for convenience, the categories should be switched in order as follows:

Digital asset					
Category 1 a digital asset that is not a Category 2 digital asset	**Category 2** a digital asset constituting a claim in respect of:				
	a moveable tangible	an immoveable tangible	a tokenised currency	an intangible financial asset[63]	an intangible non-financial asset

10. Project members noted that the **Category 2 sub-categories are helpful as a means to illustrate digital asset use cases**. However, members agreed with the Sub-Group co-chairs that, at this stage, these sub-categories **do not seem to be of significance as regards the application (or application with modification) of the principles or guidance under development by the sub-Groups** but in order to continue to test this assessment, all Sub-Group co-chairs were encouraged to consider further the sub-categories in the course of their work.

11. At the Third Session it was noted that there is no sub-category for so-called 'stablecoins', for the reasons set out in the Taxonomy note prepared for that session. Project members are also reminded that the following have not been identified as specific sub-categories of digital asset for the same reasons (i.e. because one always has to carry out a case-by-case assessment of the features of the token in question, rather than rely on its functional or marketing classification):
    - utility tokens;
    - non-fungible tokens (NFTs).

12. As follow-up points to the meeting:

    - the Taxonomy Sub-Group was requested to consider other potential taxonomical elements relating to features 'external' to the token, notably whether or not there is an issuer, whether the asset is account or token-based, and the intersection of the technology layer and any terms and conditions regarding the ecosystem in which a digital asset may be created or transferred;

    - the other Sub-Groups were invited to consider the following examples of digital assets in the context of their work, in particular to test whether any analysis or potential guidance or principles under development require adaptation to specific types of digital asset/fact pattern:

[63] The term 'financial asset' is not yet defined but it is clear from market activity that there are a wide range of examples of tokenised financial assets e.g. shares and bonds.

Digital asset					
Category 1 a digital asset that is not a Category 2 digital asset	**Category 2** a digital asset constituting a claim in respect of:				
	a moveable tangible	an immoveable tangible	a tokenised currency	an intangible financial asset	an intangible non-financial asset
Bitcoin *Mattel 'Hot Wheels' collectable NFT*[64]	*Pax Gold*[65]	*Sale of apartment*[66]	*USC*[67]	*Project Benja green bond*[68]	*Berners-Lee sale of original source code for the internet (as a NFT)*[69]

Progress since the Third Session

Information gathering exercise

13. Following the Third Session a template was developed by the Sub-Group co-chairs to support an information-gathering exercise within the Sub-Group. The overall objective of the exercise was to help gather examples of digital assets, considering the features on which Professor Kanda wished the Sub-Group to reflect following the Third Session and to describe whether (and, if so, how) features relating to the token or ecosystem in which the token exists are relevant to the principles and guidance under development by the Project.

14. Sub-Group members were invited to comment on the draft template, with members expressing wide support for the approach set out in the template. Following minor drafting tweaks to accommodate (very limited and non-substantive) member feedback, the template was issued on 23 September 2021 (see Annex A for the template) with an initial response deadline of 7 October, extended to 15 October 2021.

15. Pursuant to the template, members were invited to report, in particular, the following:
    - whether the token is Category 1, 2 or 'other' (and if the latter to explain why the token could not be considered to fall squarely within Category 1 or 2);
    - whether the token is issued (i.e. created) by an identified legal or natural person;
    - how is the token is created;
    - the rights of a person who acquires a token.

16. The responses from Sub-Group members[70] and a contribution from the Secretariat are aggregated in Annex B. The responses appear in unedited form except in the three cases in which members reported the same digital asset in which case the responses have been merged, with the exception of Binance Coin and Tether where the responses from the two members who reported that digital asset are shown separately as the responses differed in some material respects.

17. In total 23 digital assets were reported.

[64] Hot Wheels (mattelcreations.com) https://www.cnbc.com/2021/06/17/mattel-reportedly-jumps-on-nft-hype-with-hot-wheels-digital-collectibles.html

[65] https://www.paxos.com/paxgold/

[66] https://propy.com/browse/propy-nft/

[67] https://www.fnality.org/home

[68] https://stacs.io/wp-content/uploads/2021/05/Project-Benja-Public-2021.pdf

[69] https://www.bbc.com/news/technology-57474504

[70] Three Sub-Group members responded to the information-gathering exercise and reported digital assets.

18. In response to the most critical of the questions; '*Do you consider the* [features e.g. issuer, method of creation of the token, rights of the token holder] *are relevant to the Project's work and the application of the principles and guidance? If so, please explain why.',* in the vast majority of cases members responded 'no'. Where members did reflect, the following was stated:
    - Beeple and NBA Topshot: "*Personal and non-commercial use of the artwork (which is not really "granted" by issuer: such a right generally exists ex lege). The right to own and transfer the Moment.*"
    - Diem: "*Having an issuer is having an identifiable counterparty. Furthermore clarity on the contractual rights of the holders provide legal certainty.*"
    - Litecoin: "*Litecoin's main benefits are its fast transaction speeds and low fees, which makes it useful for moving funds between different exchanges or lending platforms at lower costs on networks such as Bitcoin and Ethereum. Exchanging DAs for different DAs could make the client subject to new user agreements, which in turn could impact on their rights in an insolvency.*"
    - Tether: *"Tether purports to hold USD in reserve to back the tokens, but was unable to meet client's withdrawal requests in 2017. In an insolvency therefore, clients would need protection, especially against shortfall*…."
    - digital assets (Binance Coin BNB, SwissBorg CHSB, Uniswap UNI) are not legally tethered to any right, claim or asset but are still considered as having 'value' on the basis of the use cases that are *practically/technically* made available to holders.

19. One member also wished to bring to Project members' attention that although the identities of the creators/designers of Uniswap UNI are known, it is difficult to claim that the digital assets have been issued/created by them.

20. The same member also wished to note that the classification of two digital asset (Beeple and NBA Topshot) do not appear to sit neatly in Category 1 or 2 and are interesting cases for the Project to consider.

Desk-based analysis

21. In addition to the issuance of the template and review of responses, the co-chairs have carried out desk-based analysis to inform a list of *key* features relating to digital assets and the ecosystems in which they exist which have been identified to be of relevance in considering *the legal character of digital assets*:

Feature	**Key questions**
Creation/Issuance	• How is the digital asset created? • Is there an identifiable issuer? • What is the relation between the issuer and the holder of the digital asset?
Operation	• Is there a set of binding rules between ecosystem participants in addition to the code or script that is the basis for the operation of the DLT/similar technology underpinning the ecosystem in which the digital asset exists? • Is a governing law specified in the binding rules? • Who is responsible for determining the rules and has a capacity to change them?
Storage & transfer	• What method of 'private key' storage is used: hot or cold? • Is the 'hot' storage in the context of a self-downloaded 'wallet' (i.e. no intermediary providing custodian services) or with a custodian? What are

	the terms and conditions? (On the matter of 'custody and control' see further the Questionnaire circulated to industry in the context of the Custody and Control Sub-Group.) • How are digital assets transferred? Does anything need to happen 'off-chain' in order to be perfected?
Rights	• What is the holding of the digital asset constitutive of (i.e Category 1 or Category 2)? • In relation to issuance, where there is an identifiable issuer (for Category 1 or 2), does the holder have any claim against that person in their capacity as issuer of the digital asset (or otherwise as controller of the ecosystem)? • In relation to Category 2 digital assets how is the claim established over any assets existing outside the ecosystem? What is the effect of transferring the digital asset and how is this achieved (within and outside the ecosystem)? • What are the means by which the rights can be enforced? • Can the rights be subject to change (and if so how and by whom)?

22. This list is of questions is not intended to be exhaustive.

23. The co-chairs note that any combination of answers to the questions may exist in practice and the market is ever-changing.

24. The co-chairs also note that the questions are as relevant for so-called 'DeFi' ecosystems as they are for other forms of digital asset ecosystems. In particular, it is noted that 'DeFi' tends also be used as a marketing term and careful analysis of individual ecosystems is required in order to understand the extent to which the system is decentralised (very often there are still rules of operation and/or 'controlling' or 'intermediating parties' in the ecosystem).

Reports from other Sub-Group Co-Chairs

25. In response to the request to consider the sample of digital assets referred to in the table at paragraph 9, the Secured Transactions Sub-Group co-chairs confirmed the following: *The secured transactions principles enable the creation and perfection (by control) of a security right in the digital asset but defer to the applicable law that establishes whether a digital asset embodies a right to any tethered asset. The secured transactions law does not create what we colloquially refer to as a "digital twin". If the applicable law provides that a digital asset embodies a right to the tethered asset (e.g., the Pax Gold token could be recognized as a type of a document of title), then the security right would extend to the gold as well. The secured transactions principles thus do not require any modification, at this point.*

26. Regarding the intersection with UNCITRAL work, based on information forwarded to the co-chairs on 22 October 2021, it is noted that the co-chairs understand that at this stage UNCITRAL staff are observing the taxonomy work stream which is envisaged to provide a 'legal taxonomy of digital assets' and UNCITRAL work on a wider taxonomy has been deferred at this time.

Questions to Project members for the Third Session

27. The co-chairs would welcome further reflections from Project members on the approach to the definition of 'digital asset', namely whether it is appropriate to retain the reference to 'rights' and, if so, why (and if not whether the notion of 'value' should be reflected):

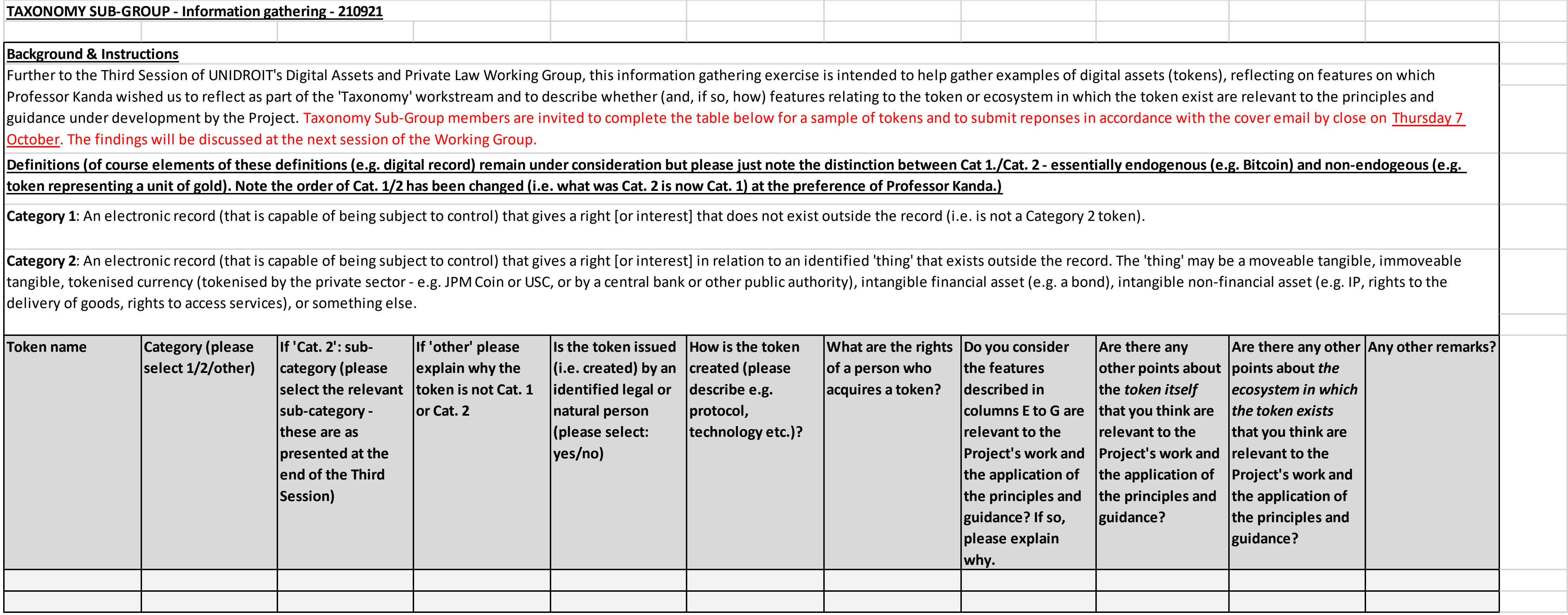
    *A digital asset is an **electronic record** which **gives rights to** the holder is **capable of being subject to control**.*

28. On the subject of the Taxonomy (and it is reminded that the Governing Council mandated the Project to produce a 'taxonomy' in the context of its work, and it seems to be generally recognised within the Project that the taxonomy is not a mere list of definitions but something to help frame the application of the principles and guidance issued by the Project):
    - Project members are invited to revisit Category 1 and Category 2 and consider the following examples of digital assets to assess if they can fit within the existing Categories or whether another category is needed (and, if so, why):
      i. Beeple
      ii. NBA Topshot

    - Project members are invited to note the limited feedback to the question '*Do you consider the* [features e.g. issuer, method of creation of the token, rights of the token holder] *are relevant to the Project's work and the application of the principles and guidance? If so, please explain why.'* In light of the limited feedback Project members are invited to consider whether these features should be further considered *in the context of the taxonomy work stream* or should be put to one side.

    - Project members are also invited to express views on whether any of the features referred to in paragraph 21 (some of which are, rightly, under consideration in the context of other Sub-Groups) are worth discrete consideration in the context of taxonomy development (and, if so, to explain why), recalling that the Project is focussed on *specific private law issues* and the taxonomy is to be viewed in this context (i.e. what is useful for the framing and application of the emerging Principles and guidance).

Annex A: Template for September 2021 information-gathering exercise within the Sub-Group



TAXONOMY SUB-GROUP - Information gathering - 210921

Background & Instructions

Further to the Third Session of UNIDROIT's Digital Assets and Private Law Working Group, this information gathering exercise is intended to help gather examples of digital assets (tokens), reflecting on features on which Professor Kanda wished us to reflect as part of the 'Taxonomy' workstream and to describe whether (and, if so, how) features relating to the token or ecosystem in which the token exist are relevant to the principles and guidance under development by the Project. Taxonomy Sub-Group members are invited to complete the table below for a sample of tokens and to submit reponses in accordance with the cover email by close on Thursday 7 October. The findings will be discussed at the next session of the Working Group.

Definitions (of course elements of these definitions (e.g. digital record) remain under consideration but please just note the distinction between Cat 1./Cat. 2 - essentially endogenous (e.g. Bitcoin) and non-endogeous (e.g. token representing a unit of gold). Note the order of Cat. 1/2 has been changed (i.e. what was Cat. 2 is now Cat. 1) at the preference of Professor Kanda.)

Category 1: An electronic record (that is capable of being subject to control) that gives a right [or interest] that does not exist outside the record (i.e. is not a Category 2 token).

Category 2: An electronic record (that is capable of being subject to control) that gives a right [or interest] in relation to an identified 'thing' that exists outside the record. The 'thing' may be a moveable tangible, immoveable tangible, tokenised currency (tokenised by the private sector - e.g. JPM Coin or USC, or by a central bank or other public authority), intangible financial asset (e.g. a bond), intangible non-financial asset (e.g. IP, rights to the delivery of goods, rights to access services), or something else.

Token name	Category (please select 1/2/other)	If 'Cat. 2': sub-category (please select the relevant sub-category - these are as presented at the end of the Third Session)	If 'other' please explain why the token is not Cat. 1 or Cat. 2	Is the token issued (i.e. created) by an identified legal or natural person (please select: yes/no)	How is the token created (please describe e.g. protocol, technology etc.)?	What are the rights of a person who acquires a token?	Do you consider the features described in columns E to G are relevant to the Project's work and the application of the principles and guidance? If so, please explain why.	Are there any other points about the *token itself* that you think are relevant to the Project's work and the application of the principles and guidance?	Are there any other points about *the ecosystem in which the token exists* that you think are relevant to the Project's work and the application of the principles and guidance?	Any other remarks?

Annex B: Aggregated responses from Sub-Group members and the Secretariat

Token name	**Category: please select 1/2/other**	**If 'Cat. 2': sub-category (please select the relevant sub-category - these are as presented at the end of the Third Session)**	**If 'other' please explain why the token is not Cat. 1 or Cat. 2**	**Is the token issued (i.e. created) by an identified legal or natural person (please select: yes/no)**	**How is the token created (please describe e.g. protocol, technology etc.)?**	**What are the rights of a person who acquires a token?**	**Do you consider the features described in columns E to G are relevant to the Project's work and the application of the principles and guidance? If so, please explain why.**	**Are there any other points about the *token itself* that you think are relevant to the Project's work and the application of the principles and guidance?**	**Are there any other points about *the ecosystem in which the token exists* that you think are relevant to the Project's work and the application of the principles and guidance?**	**Any other remarks?**
ADA (Cardano)	1			yes	ICO	Voting rights and possibility of staking	no	no	The proof of stake mechanism brings the Cardano network close to a company with ADA holders	(-)

									as shareholders	
Basic Attention Token (BAT)	1			yes	ICO	Means of payment for the advertising ecosystem realised via the Brave Browser	no	no	no	Cryptocurrency realised through a smart contract on the Ethereum blockchain (ERC20-Token)
Beeple	Everydays the first 500 days	Debateable – prob Cat 2[71]	For all intents and purposes, it would be "other", but since there are some limited rights associated with the token, there's probably an element of "intangible non-financial asset".	Strong intellectual association with Beeple's artwork, but very limited legally significant rights or claims	Yes	ERC 721 non-fungible token on the Ethereum blockchain.	Personal and non-commercial use of the artwork (which is not really "granted" by issuer: such a right generally exists *ex lege*). The right to	Yes, it probably shows how the dichotomy between Cat 1 and Cat 2 (as currently expressed) does not really express	N/A	N/A

[71] Here the relevant clause says the following (note that for the purpose of these terms the term "Digital Asset" means the underlying artwork):

				in that artwork.			own and transfer the Moment.	all the characteristics of NFTs.		
Binance Coin	1		Utility Token?	no	BNB was created with a maximum of 200 million tokens. Binance buys back and then "burns" or permanently destroys some of	Allows traders to get discounts on trading fees on Binance, can be used for payments, to book travel, for entertainment, online services,				

You acknowledge that your purchase of the **lot** means you have full ownership rights in the **NFT** itself, including the right to store, sell and transfer your **NFT**. Your purchase of the **lot** does not provide any rights, express or implied, in (including, without limitation, any copyrights or other intellectual property rights in and to) the **digital asset** underlying the **NFT** other than the right to use, copy, and display the **digital asset** for your own personal, non-commercial use or in connection with a proposed sale or transfer of the **NFT** and any other right expressly contained in these **Conditions of Sale**. For the avoidance of doubt, you do not have the right to distribute, or otherwise commercialize the **digital asset**, or to represent or imply any sort of sponsorship, endorsement, affiliation, or other relationship with the seller and/or the creator of the digital asset without the prior authorization of the **seller** or the party(ies) that holds such rights. Your rights and interest in the **digital asset** or **NFT** provided by these **Conditions of Sale** will immediately terminate upon any subsequent sale, transfer, dispossession, burning, or other relinquishment of the **NFT**.

					the coins it holds to drive demand.	and even financial services.				

Binance Coin (as reported by another member)	other	other	o The BNB token has several functions: § It offers a bunch of "perks" on the Binance platform (and its partners), § It serves as the native token for the Binance blockchain and, § In some cases, it can be used as a means of payment. § See https://www.binance.com/en/bnb and https://academy.binance.com/en/articles/what-is-bnb.	It is offered by Binance which is an identifiable commercial entity but which does not act through a clearly defined legal entity (a known problem for financial regulators).	Was created in the context of an ICO on the Ethereum blockchain. Then the token moved to the Binance chain.	Unclear. It seems like most of the use cases for the BNB token rely on Binance and its partners making things available to the holders without having any legal obligation to do so.	Yes. It's an example of a crypto that is not legally tethered to any right, claim or asset, but still has value regardless of that, on the basis of the use cases that are practically made available to holders. Particularly interesting because it's the 3rd crypto by market cap.	N/A	N/A	N/A
Bitcoin (BTC)	1			no	Permissionless DLT. The Bitcoin Protocol and its distributed blockchain consensus					

					mechanism awards new tokens to "miners" upon the solving of complex puzzles, which allows the miner to add new blocks to the blockchain.					
BNB (Binance)	1			yes	ICO	none	no	no	no	(-)
Diem (not launched yet)	2	tokenised currency (privately issued)	N/A	yes	changed to permissioned after the second WP	From WP: holders have a claim against the issuer with regards to the underlying assets held by an intermediary	Yes having an issuer is having an identifiable counterparty. Furthermore, clarity on the contractual rights of the holders provide legal certainty.	how will the redemption process go, will there be precondition for the redemption? and if there will be an freeze out period for the exercise of this right or a	contractual rights of holders against Novi the wallet	There will be capital buffers: it would be interesting to know what would be the rights of the holders on the assets representing those buffers

								delay imposed in some circumstances?		
DOT (Polkadot)	1			yes	ICO, Reward for Staking (participating in nominated proof of stake consensus mechanism)	Voting rights and possibility of participating in consensus mechanism	no	no	The proof of stake mechanism brings the Polkadot network close to a company with DOT holders as shareholders	(-)

Ethereum (Ether)	1			no	Premissionless DLT i.e. Consensus algorithm uses proof-of-stake (PoS) which allows network participants to “stake” their ether to the network, helping to secure the network and process the transactions that occur. Participants who stake their ether are rewarded ether.	owernship right on the coin	no			

Filecoin (FIL)	1			yes	ICO, Reward for participating in consensus mechanism (Proof-of-Repliction, Proof-of-Spacetime)	Payment for storage space made available via the Interplanetry File System (IPFS)	no	no	no	(-)
Gemini	2	Tokenised currency		yes	permisisonless dlt	They claim that the coin is completely backed by dollars in FDIC insured accounts				

Litecoin	1			no	Creation of litecoin tokens is done using open source, cryptographic protocol. Miners are awarded with 12,5 new litecoins per block, which gets halved every four years.	User retains the right to transact and exchange their Litecoin tokens into another currency, digital assets or cryptocurrency.	Litecoin's main benefits are its fast transaction speeds and low fees, which makes it useful for moving funds between different exchanges or lending platforms at lower costs on networks such as Bitcoin and Ethereum. Exchanging DAs for different DAs could make the client subject to new user agreements, which in turn could impact on their rights in an insolvency.			

Lofty.ai (tokenised real estate)	2	Economically, it’s an immoveable tangible. Legally speaking, it’s an intangible financial asset, i.e. membership in a LLC.	N/A	Yes	Lofty.ai generates the specific quantity of tokens related to each property. Most of the tokens are issued on the Algorand blockchain.	Each token represent membership rights in an American LLC which owns the piece of real estate.				It would be interesting to check the LLC documents. In particular, I would be interested to see what effects they attach to the transfer of the digital asset itself. What I read is that "The Lofty tokens would still represent and evidence ownership of the property contained in the LLC and, as such, could be

										transferred in the market, as needed, so long as applicable securities transfer rules are complied with”. But I would have liked to double-check the specific legal language used in the LLC docs.

Maker (MKR)	1			no	Smart Contract on Ethereum Blockchain	voting rights	No	Yes, as MKR is used to ensure that the value of a DAI is close to one USD and is therefore used to create a kind of stablecoin, this many have an impact on the legal charaterisation and treatment of USDC	The voting mechanism brings the MakerDAO close to a company with MKR holders as shareholders	Token realised through a smart contract on the Ethereum blockchain (ERC20-Token)

NBA Topshot	Individually a “Moment"	2[72]	For all intents and purposes, it would be “other”, but since there are some limited rights associated with the token, there's probably an element of “intangible non-financial asset”.	Strong intellectual association with a NBA media, but very limited legally significant rights or claims in that media.	Yes	Non-fungible tokens issued on the Flow blockchain by the NBA/Dapper Labs.	Personal and non-commercial use of the artwork (which is not really “granted” by issuer: such a right generally exists *ex lege*). The right to own and transfer the Moment.	Yes, it probably shows how the dichotomy between Cat 1 and Cat 2 (as currently expressed) does not really express all the characteristics of NFTs.	N/A	N/A

[72] o Debatable. Probably Cat 2? The Moment are intellectually/conceptually/abstractly associated to a specific media involving NBA players, but confer very little legally significant rights or interest in that media, i.e. "Subject to your continued compliance with these Terms, we grant you a worldwide, non-exclusive, non-transferable, royalty-free license to use, copy, and display the Art for your Purchased Moments, solely for the following purposes: (a) for your own personal, non-commercial use; (b) as part of a marketplace that permits the purchase and sale of your Purchased Moments, provided that the marketplace cryptographically verifies each Moment owner’s rights to display the Art for their Purchased Moment to ensure that only the actual owner can display the Art; or (c) as part of a third party website or application that permits the inclusion, involvement, or participation of your Purchased Moment, provided that the website/application cryptographically verifies each Moment’s owner’s rights to display the Art for their Purchased Moment to ensure that only the actual owner can display the Art, and provided that the Art is no longer visible once the owner of the Purchased Moment leaves the website/application.” Specifically, no industry-standard IP right in the relevant media.

PAXGold	2			yes	permissioned dlt	Holder ownership right on the underlying gold if allocated or entitlment on a specifc quantity of the unallocated gold. They could convert them into physical gold in some circumstances or into fiat	No	[As for MaKR]	what would be the rights of the holders against the intermediary?	
SOL (Solana)	1			yes	ICO, Reward for Staking (participating in nominated proof of stake consensus mechanism)	Voting rights and possibility of participating in consensus mechanism			The proof of stake mechanism brings the Solana network close to a company with SOL holders as shareholders	

SwissBorg CHSB	Debateable. Presumably 2.	N/A	The CHSB token gives its holders a variety of perks, benefits and governance rights on Swissborg's platform (see https://swissborg.com/buy-chsb), but the issuer has no legal obligation to provide these perks and benefits.	Yes, Swissborg Invest SA in Lausanne, Switzerland.	ERC20 token issued during an ICO.	No legal rights. Purchasers just trust that Swissborg will provide them with a valuable use for their tokens.	Yes. It's an example of a crypto that is not legally tethered to any right, claim or asset, but still has value regardless of that, on the basis of the use cases that are practically/technically made available to to holders.	N/A	N/A	N/A
Tether	1			yes	Creation of Tether tokens is done using transport protocols which interface with blockchains. It is a stablecoin, so all tokens are backed-up by USD. Conversion rate is 1:1.	Tether tokens are redeemable and exchangeable pursuant to Tether ltd.'s terms of services.	Tether purports to hold USD in reserve to back the tokens, but was unable to meet client's withdrawal requests in 2017. In an insolvency therefore, clients would need protection, especially against shortfall.			

Tether	2			yes	permissionless dlt	They initially claimed that coin is fully backed one to one by USD at all times- Then they changed the claim to fully backed by the reserves at all times- The proceedings with the NYAG office shown that this was not the case.	the legal classification of the legal relationship between the issuer/intermediary/ holder was particularly important here when it comes to the disclosure obligations	how will the redemption process go, will there be precondition for the redemption? and if there will be an freeze out period for the exercise of this right or a delay imposed in some circumstances?	what would be the rights of the holders against the intermediary?	Tether had frozen 33millions of tokens that were hacked and rendered them useless, this retained right of control over the coins by tether add difficulties to qualifying the legal rights of the coinhodler over its coin

Uniswap	Unclear. Presumably “other", although it could be argued that it is a Cat 1 token.	N/A	The UNI token provides its holders with the right to participate to votes and referendum related to the decentralized finance protocol Uniswap (keyword: “governance token”). See https://uniswap.org/blog/uni/.	We know the identity of the people who have created Uniwap and designed the token. For a variety of reasons, it’s difficult to claim that the token has been issued/created by them. Unclear if there is an incorporated company somewhere.	Ethereum ERC-20 token.	No legal rights as far as I know, but the technical capability to vote on the governance of the Uniswap platform. Other perks may be added in the future.	Yes. It’s an example of a crypto that is not legally tethered to any right, claim or asset, but still has value regardless of that, on the basis of the use cases that are practically/technically made available to to holders. Particularly interesting because it’s the 12th crypto by market cap.	N/A	N/A	N/A

USD Coin (USDC)	2	tokenised currency (privately issued)		yes	Smart Contract on Ethereum Blockchain	None. Coinbase initially claimed that holder can redeem the coin dollar for dollar "backed by USD in a bank account"; now the website of coinbase changed it to "backed by fully reserved assets".	One respondent said 'no'. The other said 'yes' for the following reason: Yes having an issuer is having an identifiable counterparty. Furthermore, clarity on the contractual rights of the holders provide legal certainty	yes, as USDC is a stablecoin, this may have an impact on the legal characterisation and treatment of USDC	no	Stablecoin realised through a smart contract on the Ethereum blockchain (ERC20-Token)
XPL (Ripple)	1			yes	ICO	none	no	no	Ripple is a cryptocurrency that does not use a blockchain.	(-)

Private International Law – Tentative Principles

A. Concerning the law governing acquisition and disposition (including collateralisation) of digital assets amongst adherents to the relevant digital-asset platform.

a. This law can be chosen by participants.

i. If there is no explicit choice, it is possible to revert to principles of interpretation and implicit choice. This may be particularly likely in a scenario where there are no contractual 'by laws' to the platform code.

ii. If this does not yield a result, fallback rules (such as law of the transferor, law of the transferee, etc) can determine the applicable law.

b. It is irrelevant that participants may not intend to have their transactions governed by any law at all and prefer relying on the code alone. If it comes to proceedings the court can always determine the applicable law in any case. Whether decisions would be enforceable, in practice (relevant in particular where assets are held and transferred within an un-permissioned global network), is a different question.

B. Concerning the different laws that can be relevant in an insolvency scenario:

a. General principle: the law of the jurisdiction of the territory in which the insolvent is located (COMI and similar criteria; residence and similar criteria) applies to the proceedings.

b. Tensions arise where applicable insolvency law is not the same law as the law (code?) applicable to acquisitions and dispositions on the platform. In this scenario, there is a general risk that a given transaction is regarded as final under the law (code?) applicable to acquisition and disposition (see above, A.), while the transaction, following the rules of the applicable insolvency law of the forum, could be avoided and the relevant asset would be subject to a claw-back (disregarding here any difficulties of enforcement).

i. Without clear understanding (principle? Rule?) determining whether one or the other prevails, there will be no legal certainty regarding this issue.

ii. A rule favouring the law of the insolvency and its avoidance powers may disrupt the integrity of the functioning of the digital asset platform, especially if there were participants located in different jurisdictions. Certainty of acquisition on the basis of the platforms code and rules, if any, would not be guaranteed if a claw back was possible (again, the de facto difficulty of enforcing such a claw back is disregarded here).

iii. A rule favouring the law/code applicable to acquisitions and dispositions on that platform leaves the internal functioning of the platform intact. However, it may hollow out insolvency principles of the law of the forum of any insolvency of a participant, and lead, as a consequence, to unequal treatment of creditors.

iv. This conflict could be removed or softened by

1. aligning the rules of acquisition and disposition within the digital asset platform with those principles underlying avoidance, i.e. making avoidance and claw back possible (that is a substantive question, not private international law).

2. …

C. Concerning the situation of non-native assets, where the asset has two representations, one as digital asset on the platform, and one as tangible or intangible asset outside that platform, underlying the digital asset.

a. The law applicable to the underlying asset is determined following standard rules (*lex rei sitae, lex societatis, lex contractus*, etc.)

b. The law applicable to the digital representation of the asset is described under A. and B., above.

c. Non-native digital assets require an interface, such as an intermediary organisation creating the digital token. From this point on, the PIL analysis depends on how the rights to a non-native digital assets are understood (a claim against the intermediary?). The private international law question would follow that route, e.g., if that right were to be regarded as claim against the intermediary, the chosen law would apply or, in absence of that, the law determined by the relevant fallback rules. The most relevant scenario to be considered in this context involves the outflow of the underlying asset from the estate of the intermediary, and its subsequent insolvency. A conflict may emerge under these circumstances, between the acquirer of the underlying asset with the acquirer of the digital asset, potentially governed by two different laws, see B.b.

d. It is a question of material law to make sure that these two do not start separate lives in the sense that there are to unconnected assets economically attributed to different persons. However, the question is: which jurisdiction’s law. Probably, the more viable solution is to give the law governing the underlying asset priority. This is a typical question intermediary risk, combined with cross-jurisdictional complications. Solution?