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

EN

Digital Assets and Private Law Working Group

Third session (remote)
Rome, 30 June – 2 July 2021

UNIDROIT 2021
Study LXXXII – W.G.3 – Doc. 2 (rev. 1)
English only
June 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) and Second Session (16 – 18 March 2021);

(v) Participants in Sub-Groups as part of intersessional work conducted between January and June 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, 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** contains a comparative research table summarising the use of certain terms across a number of international instruments.

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 (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)
- Kozolchyk National Law Center (NatLaw)
- *Banca d'Italia* (Central Bank of Italy)
- Law Commission of England and Wales
- *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 four sessions of the Working Group in 2020-2021:

- First session: 17-18-19 November 2020 (remote)

- Second session: 16-17-18 March 2021 (remote)

- Third session: 30 June – 1-2 July 2021 (remote)

- Fourth session: Last quarter of 2021 (tentatively November 2021)

- Fifth session: First quarter of 2022 (tentatively March 2022)

- 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

(c) Adoption by the Governing Council of the complete draft at its 101st session in May 2022.

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 will be chaired by Professor Monika Pauknerová, member of the UNIDROIT Governing Council. UNIDROIT has so far invited its Member States to nominate an expert(s) to the Steering Committee and it will be expected to start its activity once the Working Group has made sufficient progress so as to allow for a preliminary review of its work.

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 2, Appendix 4**).

38. At its second session, the Working Group mainly focused on the definition and sub-categories of digital assets and reiterated the importance of coordination with UNCITRAL regarding the taxonomy project. The WG supported a broader approach to the definition of digital assets – subject to certain exclusions – and noted the difference between that definition and the universal meaning of digital assets. The WG also noted the need for continuous review of subcategories of digital assets as the Project evolves. In future, the Working Group would need to decide whether other subcategories of digital assets should be added to the definition, and whether negotiable instruments should be covered by the Project. The Working Group is invited to consider and discuss the paper describing the scope of the taxonomy work stream which was prepared by the co-chairs of Sub-Group 4.

Note on Taxonomy (SG4)

39. This note sets out an overview of the initial scope of the taxonomy work stream and reflects discussions at the Second Session of the WG and the 'Digital Twins' Workshop.[5]

40. The Sub-Groups are 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 require adaptation to specific types of digital asset/fact pattern:

Digital asset					
Category 1 transferable code constituting a representation of:					**Category 2** transferable code constituting a representation of an asset that is not a Category 1 asset
Moveable tangible	**Immoveable tangible**	**Tokenised currency**	**Intangible financial asset**	**Intangible non-financial asset**	
Pax Gold[6]	*Sale of apartment*[7] [For now, let us consider 'whole' real estate only (shares of moveable tangibles would be 'intangible financial assets')]	*USC*[8]	*Project Benja green bond*[9]	*Berners-Lee sale of original source code for the internet (as a NFT)*[10]	Bitcoin *Mattel 'Hot Wheels' collectable NFT*[11]

Context

41. The Project is intended to develop principles and legislative guidance in the area of private law and digital assets.

---

5 31 May 2021.

6 https://www.paxos.com/paxgold/.

7 https://propy.com/browse/propy-nft/.

8 https://www.fnality.org/home.

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

10 https://www.bbc.com/news/technology-57474504.

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

42. The taxonomy will inform and accompany this work but may also be applied by UNIDROIT-UNCITRAL for other (as yet unspecified) purposes. It is intended to highlight the characteristics of digital assets and the system in which they exist (for example, any rules prescribed in the system's protocol[12] (if any)) that may give rise to some of the legal challenges addressed by the principles and legislative guidance. Put another way, **some of the principles and legislative guidance may be relevant only to one or more sub-categories of digital assets, or may require modification in their application to some types of digital assets**. Therefore, the taxonomy will need to identify such sub-categories as are needed for the Project thereby forming **the navigational tool to guide readers** to the relevant sections of the principles and legislative guidance depending on the type of digital token at hand. For the avoidance of doubt, this is not the same as providing a taxonomy of all digital asset for 'universal' purposes.

43. The taxonomy is not to be considered the same thing as the list of definitions to be used for the principles and guidance, but we will need to follow closely and contribute to terminology used by other work streams and ensure that the definitions are consistent with the taxonomy and coordinated.

44. The taxonomy is likely to remain a 'live' beast during the course of the Project.

Overarching principles

45. In so far as possible the taxonomy should be:

- technology neutral
- future-proof

Scope – 'digital asset'

46. The intention, as confirmed at the Second Session, is to start broad.

47. Accordingly, there is agreement that the use of cryptography should not be a characteristic delineating what is in or out of scope of the Project's work.

48. Additionally, it has been agreed that the mode of issuance should not be considered a core delineating feature. Nor should regulatory classification (e.g., 'security' or 'financial instrument' under relevant regulation), albeit this will need to be kept under review as, in some cases, the Project may conclude that existing principles apply and do not need adaptation to certain types of instrument that happen to take the form of a digital asset (as would be a 'technology neutral' conclusion).

49. As the scope of the work is not referring to 'digital unit' (pure code), rather 'digital *asset*', there is agreement that 'asset' must have some significance. For this reason, it is assumed that the Project's work is focussed on digital assets that are *constitutive* of something (e.g., value, right, claim) rather than *purely evidentiary* but this is a tentative assumption.

50. At the Second Session, there was some discussion as to whether a definition of 'digital asset' developed for the purposes of the Project should refer to 'value', 'rights' and/or 'claims'. There was agreement that 'claim' encompasses 'rights' therefore there is no need to refer to both terms. As to 'value', this was observed to be used in definitions applied by international standard-setters active

[12] For instance, a 'blockchain protocol' setting out a binding set or rules between the system participants in addition to the code that provides the technical functionality for the system.

in this field, including the FSB[13] and FATF.[14] Although imperfect, there was agreement that 'representation' is a term that can be used on a working basis to link the code to the 'value'.

51. There was general agreement that tokens such as gaming tokens, and 'loyalty' points schemes and airmiles should be carved out of scope.

52. In view of these observations, the following definition of 'digital asset' is proposed for the Project's work and as the 'umbrella' term for the taxonomy work stream. The need for specific exclusions from the definition, depending on the overall scope of the Project's work, can be kept under review.

> **'Digital asset' is a:**
>
> ***digital representation of value which can be used for payment or investment purposes.***

Sub-categorisation of 'digital asset'

53. The term 'digital asset' covers a vast range of cases – some where the value is limited to and actionable in the purely digital sphere, and others which exist or are actionable 'off chain' (sometimes referred to as 'real world' assets though this term may be confusing). This distinction is of the utmost importance for the Project's work, for instance a question of whether the transfer of the digital asset would result in the automatic transfer of the 'off chain' asset as a matter of property law.

54. As such, and as discussed at the Second Session, one can anticipate **two basic sub-categories of 'digital asset'** (essentially leveraging the 'native' vs 'non-native' categorisation with an aim to avoid the terms as the Sub-Group recognises these terms have a particular use by technicians in the sphere of digital-asset development):

- **Category 1**: transferable code constituting a representation of:
  - (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[15])
    - central bank digital currency (CBDC)
  - (iv) an intangible financial asset
  - (v) an intangible non-financial asset (e.g., IP)
- **Category 2**: transferable code constituting a representation of an asset that is not a Category 1 asset.

55. Category 1 has been sub-categorised by reference to the type of asset to which the claim relates. These sub-categories are helpful in illustrating why certain of the principles or guidance may be relevant only to certain types of digital asset (e.g., in the context of enforcement).

---

[13] The FSB uses the following definition of 'digital asset' (as compared to 'crypto-asset' which it defines differently: *A digital representation of value which can be used for payment or investment purposes. This does not include digital representations of fiat currencies*. https://www.fsb.org/wp-content/uploads/P131020-3.pdf

[14] FATF uses in its Standards and guidance the term 'virtual asset': https://www.fatf-gafi.org/publications/virtualassets/documents/virtual-assets.html?hf=10&b=0&s=desc(fatf_releasedate). *"Virtual asset" is a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities, and other financial assets that are already covered elsewhere in the FATF Recommendations.*

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

56. 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).

57. As for so-called 'stablecoins', as explained at the Second Session, the Sub-Group has discarded the consideration of these digital assets as a free-standing category of 'digital asset'. So-called 'stablecoins' comprise an incredibly mixed bag of things. As observed by the Financial Stability Board (among very many other international standard-setters), 'stablecoin' is primarily a marketing term and cannot be relied upon for any legal, regulatory, or other purpose. As the FSB put it in the most recent (October 2020 report):[16]

> *The term stablecoin commonly refers to a crypto-asset that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets. In turn, the value of these assets typically determines or affects the market value of a stablecoin. A stablecoin may also employ algorithmic or other means to stabilise or impact its market value by, for example, automatically adjusting its supply in response to changes in demand.*
>
> *There is no universally agreed definition of stablecoin. The term stablecoin does not denote a distinct legal or regulatory classification. Importantly, the use of the term "stablecoin" in this report is not intended to affirm or imply that its value is necessarily stable. Rather, the term is used here because it is commonly employed by market participants and authorities.*

58. To illustrate the range of tokens called 'stablecoins' one can compare:

- JPM Coin (in circulation) – holders have 1:1 claim against the bank (Coins are pre-funded with deposits)
- Diem (proposed) – entitlements of holders not yet confirmed but expected to provide a claim against the issuer in relation to a reserve of assets held with custodian banks in the form of deposits and investments in government bonds
- Dai (MakerDAO) – pegged to USD but collateralised with other crypto-assets held in vaults 'on chain'
- Non-collateralised tokens kept 'stable' in value (e.g., pegged to USD) through the use of algorithms (e.g. Basis which never got off the ground)

59. Similarly, the following have not been identified as specific sub-categories of digital asset:

- so-called **utility tokens** (essentially representations of a one-off right to access a good or service) would be likely to be Category 1(v) (but potentially could be Category 2 –a case-by-case assessment is needed);
- **non-fungible tokens** – as illustrated in the table, NFTs may be Category 1 or 2 depending on their features and, again, a case-by-case assessment is needed.

60. Finally, the Sub-Group notes that in addition to characteristics of different types of digital assets, there may be other features that are relevant to the navigational taxonomy referred to in paragraph 3, for instance factors 'external' to the assets themselves. This point will remain under review by the Sub-Group as the taxonomy work progresses.

Applying the categories in practice

61. In terms of next steps, building on the examples discussed at the 'Digital Twins' workshop, and wider desk-based market analysis, **it is suggested that Sub-Group provide further examples of 'digital assets' falling within the categories identified above**. This exercise will support an analysis of whether further sub-categories of Category 1 are needed, and whether Category 2 could (or should) be sub-categorised.

---

16 https://www.fsb.org/wp-content/uploads/P131020-3.pdf.

Digital asset					
Category 1					Category 2
Moveable tangible	Immoveable tangible	Tokenised currency	Intangible financial asset	Intangible non-financial asset	

62. **For the other Sub-Groups, it is relevant to consider whether the above categories and sub-categories make any difference for the purposes of the legal analysis or principles identified in their Sub-Groups.** In some instances, the answer is likely to be 'no', in other cases, Sub-Groups are encouraged to refer to the relevant category/sub-category in their analysis and signpost clearly where sub-classifications of digital assets are relevant. **To facilitate this exercise, it is proposed that the Sub-Groups use the digital assets referred to below as examples of the relevant category/sub-category:**

Digital asset					
Category 1					Category 2
Moveable tangible	Immoveable tangible	Tokenised currency	Intangible financial asset	Intangible non-financial asset	
Pax Gold[17]	*Sale of apartment*[18] [For now, let us consider 'whole' real estate only (shares of moveable tangibles would be 'intangible financial assets')]	*USC*[19]	*Project Benja green bond*[20]	*Berners-Lee sale of original source code for the internet (as a NFT)*[21]	*Bitcoin* *Mattel 'Hot Wheels' collectable NFT*[22]

63. **Finally, members of the Project are invited to comment on the categories referred to in paragraph 54**.

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

64. 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.[23] 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

17 https://www.paxos.com/paxgold/.

18 https://propy.com/browse/propy-nft/.

19 https://www.fnality.org/home.

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

21 https://www.bbc.com/news/technology-57474504.

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

23 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.

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.

65. 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.[24] 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).

66. 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.

67. 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.

68. 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).

[24] 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.

Illustrations

Non-fungible Tokens (NFTs) – NBA Top Shot

69. NBA Top Shot[25] 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

70. 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 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.

71. 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

72. Wrapped Bitcoin[26] 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)[27]

73. 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

---

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

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

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

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.

Question for the Working Group: Should DeFi be considered a category of "digital twins"?

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

74. 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.[28] 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

75. 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.

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

[General comment:

a. 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 interests in digital assets—i.e., matters that are and that are not covered by the principle—and thus to the scope of the digital assets law.]

b. 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 (i.e., the digital assets law) are to laws of general application that do not address specifically digital assets.

(1) The applicable law other than law governing digital assets contemplated by these principles (i.e., 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 interests in digital assets. (As used in this principle references to proprietary interests include rights with proprietary effects.)

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

(3) The law should define the transfer of a digital asset as the change of a proprietary interest 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).

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

*[**Comment 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.][29]*

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

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

(b) whether a person has validly transferred a proprietary interest 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 (i.e., "third-party effectiveness").

[**Comment 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 interests (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)).]*

(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 and indirect 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 [see Principle C and Principle X].

(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.

***[Comment 3.** Paragraph (7) reflects the view that the law should provide choice-of-law rules relating to digital assets. Subgroup 2 has not, however, 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.]*

[29] This comment is similar to Comment 2 in the draft Control principle. 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 the other.

(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 innocent acquisition rule (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 interests (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.

[Comment 4. *The rights conferred on IAs in accordance with subparagraphs (a) and (b) mean that digital assets will have attributes similar to those of negotiability under rules applicable in some jurisdictions to negotiable instruments, negotiable documents of title, and negotiable certificated securities.]*

(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 interest in a digital asset or derivative digital asset even if control of the IA is changed by a person that has no proprietary interest in the digital asset and that is acting wrongfully.

[Comment 5. *Subparagraph (d) 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 Comment 3 in the draft Control principle.]*

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

(vii) the test adopted in the Geneva Securities Convention, Article 18(1), i.e., 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) The law may, consistent with these principles, address other issues relating to proprietary interests in digital assets.

2. Definition of Control

76. The Working Group discussed a connection between control and custody, as well as the importance of progress on questions relating to secured transactions and applicable law. Whereas the term "exclusive" has not been fixed, the Working Group discussed that exclusivity may be just one element of control and can mean control by more than one person. The Working Group also agreed to discuss potential substitution of functional term "power" with term "ability" (see **Annex III** which contains a comparative research table summarising the use of certain terms across a number of international instruments), which may provide more clarity if properly defined, and agreed to further distinguish on-chain and off-chain assets with regard to control.

PRINCIPLE [X.1]
"Control"

[General comment: Purpose and role of "control"

a. 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 and as a method of third-party effectiveness (perfection) [and as a basis of priority] of security rights in a digital asset. States also may adopt the concept of control as an element of third-party effectiveness of proprietary interests more generally. In this respect control assumes a role that is a functional equivalent to that of "possession" of movables. For this reason, 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, we refer to "possession" in this context as a purely factual matter and not as a legal concept.

b. The change of "control" from one person to another person must be distinguished from a transfer of proprietary interests or rights with proprietary effects. A change of control may or may not be associated with a transfer of such rights. This is an example of the "control" of a digital asset operating as a functional equivalent of possession of movables. In an effort to highlight this distinction between changes of control and transfers of proprietary interests, earlier drafts of this principle have variously referred to a "transfer of control," a "delivery," and a "delivery of control." This draft refers simply to a "change of control." The Working Group may wish to consider whether this approach is adequate.

c. 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 (i.e., administer) digital assets for its [clients] [account holders]. The private law (as well as a regulatory framework) may require a custodian to maintain "control" of digital assets held for [clients] [account holders]. This is an example of one person (the custodian) having control while proprietary interests remain with another person (the [client] [account holder]). A thief of digital assets would be another example of the separation of control and ownership interests.]

(1) The [definition] [attributes] of control should include the following criteria:

(a) subject to paragraph (3), the digital asset or the relevant protocol or system confers on a person in control of a digital asset:

*[**Comment 1.** In the following provisions of subparagraph (a) the term "ability" replaces the term "power" used in some earlier drafts of the Control principle. While the terms have identical meanings, "ability" is more compatible with the concept of control as a factual standard in subparagraph (1)(a) and "power" has a more "legal" connotation. On the exclusivity aspect of an ability, see Comments 2 and 3.]*

(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 [exclusive] ability to obtain substantially all the benefit from the digital asset; and

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

[Comment 2. *The Working Group may wish to consider whether the ability specified in paragraph (1)(a)(iii) must be exclusive. For this reason, the term "exclusive" appears in square brackets in that provision. 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 permitted another person (or persons) to obtain the benefit. It also may be that this situation is covered by the exceptions provided in paragraph (3), in which case the square brackets may be removed. In any event, a control person need not prove a negative, as provided in paragraph (4) and explained in Comment 4.d.]*

(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.

*[**Comment 3.** Paragraph (2) addresses the situation in which the change of control relates to a derivative digital asset over which control is acquired and that 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.]*

(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). 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.

*[**Comment 4.***

a. The exclusive ability requirements in paragraph (1)(a) (as relaxed in paragraph (3)) recognize that the ability to exclude is an inherent aspect of proprietary interests. However, it is possible that a person other than a person rightfully in control 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.

b. 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 persons for purposes of convenience, security, or otherwise.

c. 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.

d. 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) 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.*

e. 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.

f. The exclusivity criterion (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 (subject to understood exceptions) and in fact that generally has been the case.]

(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.

3. Provision of digital asset custody services

77. At its second session, the Working Group clarified that the definition of "control" was a factual instead of a legal definition. The WG noted the potential influence of different definitions of control on duties of custodians, and the importance of differentiation between holding by custodians and exchanges in the scenario of an outright transfer model. The WG also discussed a shared control scenario and confirmed that recordkeeping should be defined in functional or factual terms and would be one of the core parts of the Principle.

78. The WG agreed to further consider the Control Principle in relation to custody in light of development of illustrations of use cases, as well as issues relating to pooled accounts along with segregated accounts, custody on non-fungible DAs, custodian insolvency, custody with regard to digital twins, custody of both direct and indirect holding scenarios.

Principle C – Custody

Revised version of 17 June 2021
Text that is new or revised since the meeting on 2nd June is in green.

Custody and other situations

This Principle applies to custody, i.e., 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 would carry 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 custody of a digital asset, which involves two persons (the custodian and the client for whom the custodian holds the asset), must be distinguished from four other situations:

[Direct] holding. An investor is the holder of a digital asset when, by using some hardware, software, or online service, she controls the asset. 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. This service is therefore not a custody service as defined in this principle, even though it is sometimes called "custody" by market participants. It is, instead, a form of direct holding. In contrast, where a business provides a custody service, its clients transfer their digital assets to addresses or private keys controlled by that business. [NOTE: This paragraph has been the subject of a long and not

uncontroversial discussion in SG1. The current draft represents the view of the majority of the group.]

Personal obligation to deliver a digital asset. A Fintech firm or a financial institution (or any other business for that matter) may incur an obligation to deliver a certain quantity of a given digital asset (such as cryptocurrency) 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. Because its obligation to the client must appear in some form on its balance sheet, the firm or institution is likely to 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. Whether or not there is such an account, the investor does not have control of digital assets; she merely has an unsecured personal claim against the obligee. If the obligee 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. This situation is further addressed below in principle C.8.

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.

Open Question #1

Is it correct to distinguish smart-contract control from the other four situations? What is the legal analysis? Is that a unique situation where some form of property is not controlled, possessed, and owned by one or more natural or legal persons?

Are there situations where a DAO provides custody services (as defined in this principle)?

Open Question #2

Do these descriptions apply equally to fungible and non-fungible digital assets? While the distinction will hopefully be addressed by the taxonomy group, we note provisionally that whether certain assets are fungible is often a matter of commercial usage but ultimately relies on the agreement between the relevant parties. Bitcoin and other similar assets are usually treated as fungible. Conversely pictures or songs embedded into or linked to a so-called non-fungible token (NFT) are usually treated as unique (non-fungible), even though they are publicly accessible and copied and stored by an unlimited number of users.

C.1 A person who has control of a digital asset in accordance with Principle [X] Control is a [holder] [control person] of that asset.

Explanation

The word [‘holder’] [‘control person’] is used to indicate a person for whom a set of facts is true, that set of facts amounting to control of the digital asset. There is a need for a

word to describe such a person to make drafting of the Principles easier. However, since the concept of 'control' in Principle [X] Control is purely factual, this word is also purely factual. Whether the [holder] [control person] has any proprietary interest in the digital asset, and the nature and strength of that proprietary interest, is a matter for the applicable law, as set out in Principle X.2(4).

If the [holder] [control person] is a corporate entity, the fact that several officers or employees must act jointly to transfer a digital asset does not create joint holding: the corporate entity is the only [holder] [control person] of that asset.

Note that, while principle C.1 falls within the remit of SG1, it does not belong eventually within the Custody Principle as its ambit is more general. It probably should go in a general section at the beginning of the Principles.

[Open Question 2A for SG1: In the commentary to Principle X the term 'control person' is used. We have put this in square brackets as alternative to 'holder', although we (Luc and Louise) prefer 'holder'. The verb 'hold' has been changed to 'control' in the paragraphs of the principle for consistency with Principle X. Where the verb relates to the relationship between the custodian and the client, rather than the factual control of the asset (Principle X) both terms have been placed in square brackets for now.]

C.2 This Principle applies to a person providing or agreeing to provide custody services in the course of a business (hereafter referred to as a custodian).

Explanation

The provisions in this Principle are reserved for persons providing the service of custody (as defined in principle C.3) on a professional basis. The service may be provided in addition to other services relating to digital assets (trading, lending…). While a professional custody is likely to be subject to some licensing and other regulatory requirements, the legal, operational, and regulatory set-up of the custodian does not matter to the application of the Principle.

C.3 A person (known as the custodian) provides custody services in relation to a digital asset to another person (known as the client) if:

(a) the custodian has or must obtain control of the asset, or another custodian (the sub-custodian) has or must obtain control of the asset [and provides custody service to the custodian in relation to that asset] [is bound to the custodian by the duties in this paragraph];

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

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

(d) 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.

Explanation

The language of principle C.3 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.3 is definitional of the duties which are owed by a person providing custody services [under an agreement with a client]. Thus, if the duty to obtain control of the asset in C.3(a), and the duties in C.3(b), (c) and (d) are not owed, the service provided is not custody.

(a) Includes in this definition the inability of the custodian to use the asset for its own benefit except as permitted by the client or by law. The client may consent to that use either by contract or by an instruction to the custodian.

(b) Makes the basic point that a custodian is a person who must deal with the assets according to the client's instructions

(c) Merely states that a custodian owes some duties. These are elaborated in principles C.5 and C.6.

Principle C.3 does not require that a custodian is the sole [holder] [control person] of the digital asset in its custody. There could be joint control granted to the custodian and its client, provided that the client cannot transfer the asset without the consent of the custodian. But the client's sole control over the asset would render it impossible for the custodian to discharge its duties and therefore would not qualify as a custody relationship.

Open Question #3

Besides "except to the extent permitted… by the client" in C.3 (a), should this Principle deal more extensively with the right of use and its exercise? Inter alia, should it address possible limitations to granting the right of use, certain duties of the custodian's when exercising that right, or the treatment of the client's claim for return of the asset when the custodian becomes insolvent?

C.4 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.

Explanation

Principle C.4 makes it clear that the client could (in the relevant jurisdiction) hold the asset on trust for someone else (e.g., could be an investment fund) or the functional equivalent could occur in other jurisdictions. Principle Y only addresses the first relationship in the chain.

We have been asked by the Working Group to look beyond the first tier (custodian-client) relationship and to consider a longer chain of holding. Principles C.9 and C.10 are our first draft to address the issue of sub-custody, together with some amendments to C.3.

C.5 The duties owed by a custodian to its client may include:

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

(b) the duty at all times to secure, and to maintain, effective control of digital assets of the kinds and in quantities identical to 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 controlled for the account of clients separate from assets controlled 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 controls that asset.

Explanation

Principle C.5 sets out duties that a state may include. It assumes that a custodian records the assets controlled for its clients in accounts (records which may exist in any form, digital or otherwise). Maybe the duty to keep proper records should be included in this principle, in addition to the duty to hold assets correlating to those records.

(a) A custodian must maintain a record of the digital assets it controls 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 control assets correlating to those records. Thus, if the record shows that a custodian [holds] [controls] 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 (i.e., 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] [controls] assets for a number of clients. [NOTE: omnibus holdings were present in the MountGox and Cryptopia cases]. 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. Instead, the number of assets the custodian [holds] [controls] for each client is recorded in the books of the custodian. This enables an exchange, for example, to transfer assets from one client to another in its books without doing any transaction on chain. 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 on chain. If the digital assets are non-fungible, they can only be [held][controlled] 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.

Open question #4
Should we include a description of a pooled account and a segregated account? Is the draft description correct? If not, how should it be changed?

C.6 A digital asset controlled for a client by a custodian

(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.

Explanation

Principle C.6 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'.

C.7 A person who controls a digital asset is not a custodian of that digital asset merely because it maintains an account in the name of a client and is obliged to transfer that asset or an equivalent asset to that client or another person.

Explanation

Principle C.7 refers to the situation discussed in the introduction under "Obligation to deliver a digital asset". A dealer may maintain an account of the digital assets if it buys and sells for a client without assuming the position of a custodian. An exchange or trading platform may record its participants' assets in client accounts without assuming the position of a custodian. In such cases, the dealer or the exchange is not acting as a custodian and the digital assets are controlled on its own account. The accounts maintained in the name of clients record the dealer's or exchange's obligations to each client and these obligations must be reflected in its balance sheet. As mentioned above, the consequence of this situation is that, on the insolvency of the dealer or exchange, the client is an unsecured creditor as it only has a personal claim against the insolvent

party. A State may consider whether regulation is required to provide protection to some or all types of clients.

Whether a dealer, a trading platform or another person has an obligation to deliver digital assets to a client or whether it holds these assets as custodian for its client is a matter of agreement between them and must be determined on the circumstances of the case. It may well be that a dealer or a trading platform offers both possibilities to its clients. In some situations, it will not be clear from the agreement which possibility is the correct analysis. Here, a court would have to look at various factors to determine the correct analysis, such as whether the dealer or trading platform is regulated as a custodian, describes itself as a custodian, whether it accounts for the digital assets on its balance sheet, and whether it has a very extensive right to use the assets with no or very few limitations.

C.8 If a person enters insolvency proceedings, a digital asset that it controls as a custodian for the account of a client does not form part of that person's assets for distribution to its creditors.

Explanation

This paragraph 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][control person] is not a custodian, any assets it controls will be part of its assets for distribution to its creditors.

Open Question #5
Do we need to address the issue of shortfall in this Principle?

C.9 When authorised by a client or by law, a custodian may control a digital asset for that client through another custodian (a sub-custodian) if the sub-custodian is bound by the duties stated in principle C.3.

C.10 When a custodian controls 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 controlled as custodian for its clients do not form part of the custodian's assets for distribution to its creditors.

Explanation

These two principles relate to the situation where an entity (A) provides custody services, as defined in C.3, without itself being the [holder] [control person] of the digital asset. Instead, another entity (B) provides custody services to B, acting as a sub-custodian. B is the [holder] [control person] of the digital asset as defined in C.1, since it is B that controls the digital asset. The principles are designed to ensure that A's client is not disadvantaged by the use of B as sub-custodian, compared to the position where A itself is the [holder] [control person] of a digital asset that is the subject-matter of the agreement for A's provision of custody services.

4. Taking of security over digital assets

79. At its second session, the Working Group primarily focused on the use cases, illustrations, and Principles A-D on secured transactions. On the scope of the Principles, the Working Group agreed to start out broadly and reiterated that the Principles should be drafted on the basis of legal system neutrality 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).

80. The Working Group agreed to further: (i) explore possible modification of Principle A for greater adaptability for civil law systems; (ii) re-examine the use of "any" in Principle B, which raises

the question as to whether all digital assets are amenable to collateralisation; (iii) provide clarity by distinguishing between the legal and factual in respect with the phrase "power to transfer" in Principle C and its comments. The Working Group agreed that further discussion and research would be needed regarding the broad matter of "digital twins" and their use as collateral.

Note on Secured transactions (SG3)

81. 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 **six illustrations**, **special sections on digital twins and secured transactions and on DeFi (decentralized finance)**, **a series of six draft principles** together with commentary, found below, for the consideration of the Working Group.

OUTPUT

82. The project is to formulate principles of private law for digital assets (DAs). Principles are high-level formulations that justify a rule, but they do not necessarily prescribe a directive. Standards and legislative recommendations are more concrete. Some principles may need to be more concrete, such as on control, others just restated (e.g., a person may create a security right in any rights and powers it has), and an explanation provided how they would apply to security rights in digital assets. Several models for the principles have been mentioned, including the UNIDROIT "Netting Principles" (https://www.unidroit.org/instruments/capital-markets/netting). A useful model in terms of structuring our output may be the ALI-ELI Principles for Data Economy that consist of: 1) black-letter principles; 2) comments; 3) illustrations; and 4) (comparative) notes.

COORDINATION

With other SGs:

- SG1 (Holding)
    - Defining "control" for the purpose of establishing custody
    - Holding of DAs and any tethered "real-world" assets [consistently with the approach taken in the other SGs, this aspect is deferred]
    - Custodians right to use and re-pledge DAs
- SG2 (Transfers)
    - "Control" as a method of transfer and resolving competing claims
- SG4 (Taxonomy and conflict of laws/private international law rules)
    - Taxonomy i.e., classification of DAs (from a private law perspective rather than a regulatory one)
    - Conflict of laws/private international law rules in relation to security rights in DAs

With other projects

- UNCITRAL
- UNIDROIT
- Enforcement: Best Practices (https://www.unidroit.org/work-in-progress/effective-enforcement-best-practices)

- Model Law on Warehouse Receipts (https://www.unidroit.org/work-in-progress/model-law-on-warehouse-receipts)

FOCUS OF SG3'S WORK

83. The charge of SG3 is to address the issues and questions set out in Part D 6 of the Issues Paper (Study LXXXII – W.G.1 – Doc. 2). The suggestions included below are for discussion, and the Working Group members are invited to provide additional suggestion or propose to delete some of the ones listed below. The objective of SG3 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.

MODELS FOR INSPIRATION:

84. SG3 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.

SPECIAL SECTIONS

Security rights and digital assets that embody real-world assets

85. The Project considers several types of digital assets that embody, or evidence, various real-world assets, whether tangible or intangible. Modern secured transactions laws provide for rules applicable to specific types of assets (e.g., negotiable documents, securities, etc.), but do not define 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 in an applicable law to be used as collateral. This sub-section describes how negotiable documents came to be recognised as embodying rights to goods, thus acquiring the quality of being able to transfer security rights to a creditor.

86. 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.

87. 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.[30] 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.[31] This approach is followed in, for example, South Africa[32] and Australia[33] 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.

88. 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".[34] The "right of control" is defined as "the right under the contract of carriage to give the carrier instructions in respect of the goods",[35] while "controlling party" is defined as "the person that … is entitled to exercise the right of control".[36] 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.[37] 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.[38] 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

---

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

31 See e.g.., *The ''Future Express''* 1992 2 Lloyd's Rep 79 at 96.

32 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.

33 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.

34 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.

35 Article 1(12) of the Rotterdam Rules.

36 Article 1(13) of the Rotterdam Rules.

37 Article 50(1) of the Rotterdam Rules.

38 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).

electronic transfer record will then have the same effect as that of delivery of a "paper" transport document.

89. 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[39] and the Netherlands.[40] Even in such cases, the legislative recognition was usually preceded by mercantile practice and other developments.[41] Statutory recognition can also be employed to recognise documents of title in digital format.[42] This is presently the case with respect to the implementation of the UNCITRAL Model Law on Electronic Transferable Records.

90. 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."

91. 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.[43] 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.[44] This way of dealing with physical goods transported by sea developed for the sake of convenience.[45] 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.[46]

92. 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

---

[39] 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.

[40] 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).

[41] 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.

[42] 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).

[43] *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.

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

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

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

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.[47] 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.[48]

93. 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".

94. 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*."

95. 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.

96. 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.[49] 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.

Prevailing DeFi practices and features

Introduction

97. "DeFi" refers to Decentralized Finance, which combines various technologies that collectively provide decentralized or disintermediated means of executing traditional financial transactions using

---

[47] 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.

[48] 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.

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

crypto assets.[50] 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.

98. 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.

99. 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.*

100. 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.

101. 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.

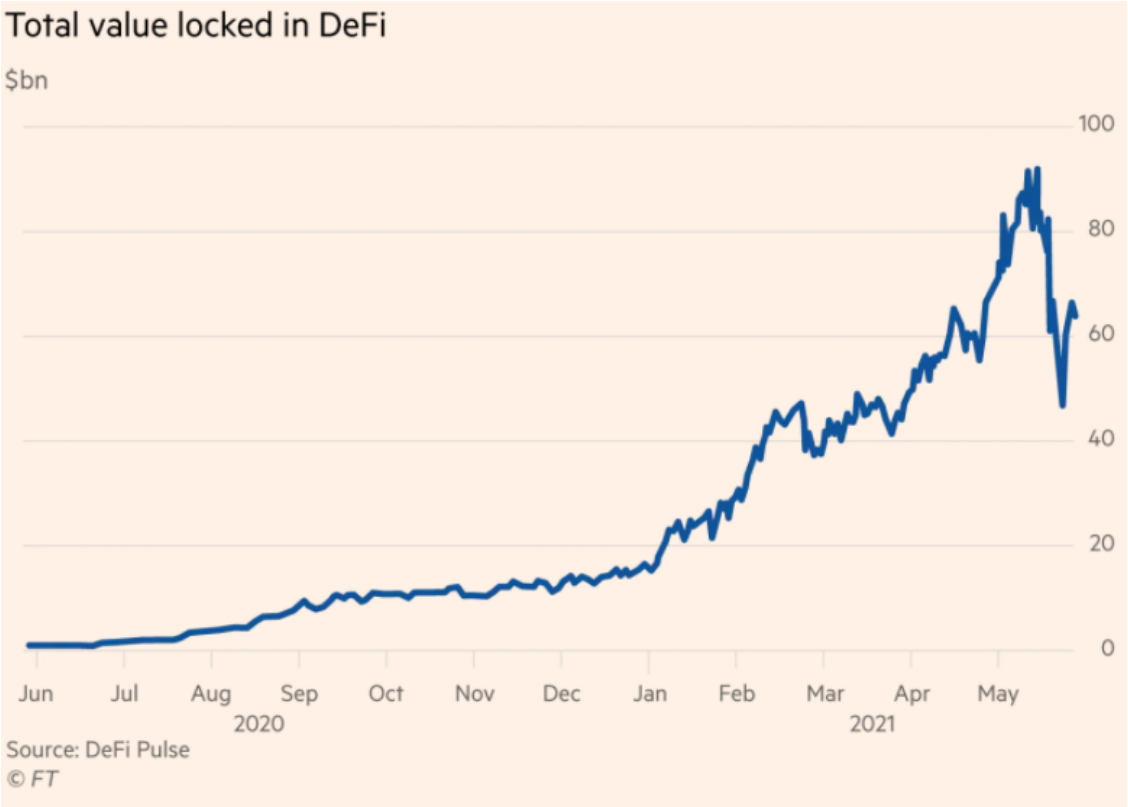
102. The DeFi sector is growing and the value of digital assets therein is rapidly increasing. According to data from DeFi Pulse and FT[51], the value of cryptocurrency being used as collateral for loans and other transactions with DeFi providers has recently reached the amount of $67bn.

---

[50] "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.

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

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:



Description of DeFi services

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

"Depositing" services

104. 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 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.

105. 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.

106. 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

107. 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.

108. 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.

109. 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

110. 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.

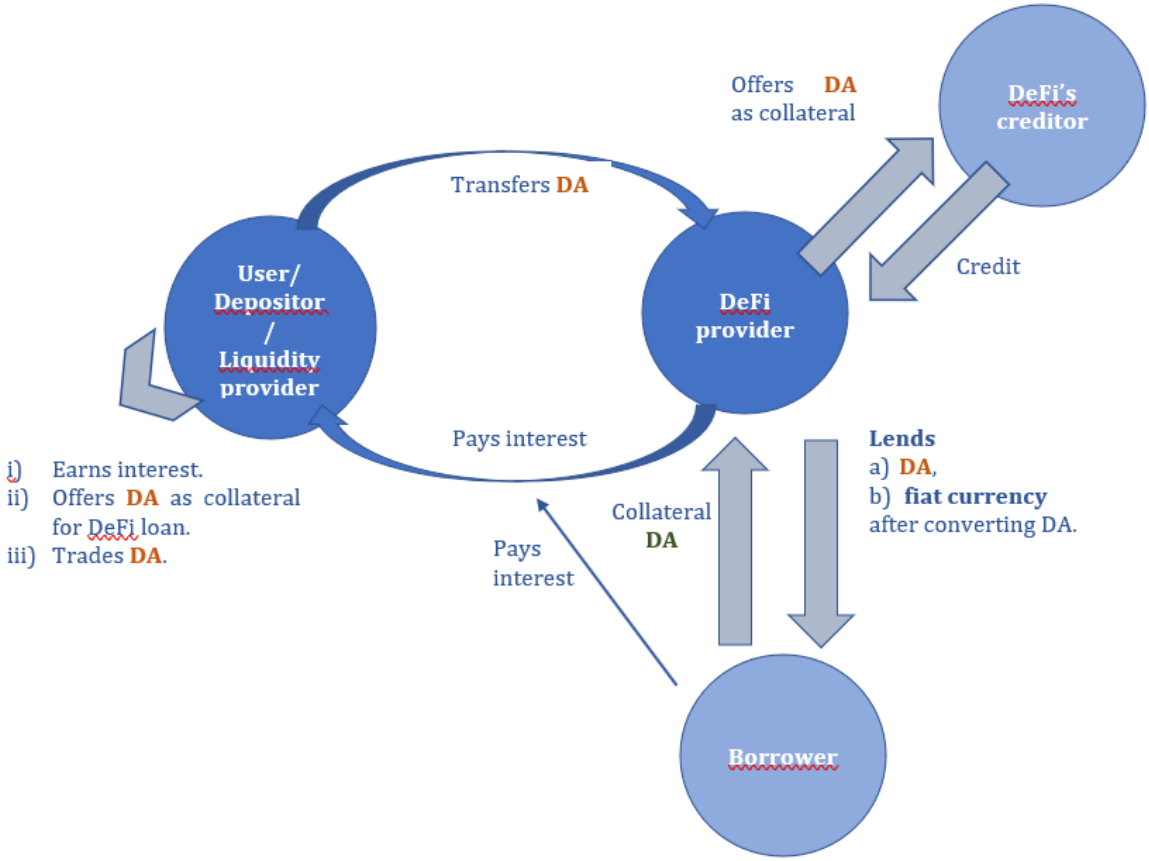
111. Each LP holds a pair of assets; the ratio of asset to asset becomes the "price" for a trader. For example, if a pool holds 5,000 x coin and 500 y coin, the trading price at that time would be 10 x coin to 1 y coin. If a user wishes to provide additional liquidity, they would be required to contribute

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.

112. 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.

113. 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

114. 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.

Example 2

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.

Example 3

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…

Example 4

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.

USE CASES

115. DAs are already used in several types of collateralized transactions, and structures are being designed to enable their use in the near future. Since the Principles are to be forward-looking, it is necessary to examine various illustrations of existing and prospective use cases. This section provides concrete illustrations to aid the discussion of the specific 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 functions. Even though they may generally fall outside the scope of secured transactions laws, given that they provide recourse against some asset without legal formalities, 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

116. The MakerDao system is an online service provider using smart contracts deployed on the Ethereum blockchain that allows users to create structures that function like collateral transactions. Users surrender control of digital assets that are used as "collateral" by the system. Users then 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, relative to some other asset).[52] The newly created stablecoins are, by design, always over-collateralized and resemble loans of property. If the ratio of the value of the withdrawn stablecoin to the value of the collateral hits a limit, the collateral can be liquidated using a semi-automated process. A user can also provide an amount of the

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

stablecoin back to the system to reclaim their "collateral". The smart contracts automate 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. No legal contracts or legal compliance are included in the system or required to use the system. No traditional intermediaries are involved in the operation of the system.

Illustration 2: Borrowing of Digital Assets

117. Participants in the market 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 assets. Multiple centralized and decentralized platforms offer various types of "lending" to holders of digital assets. Some participants will take control of those digital assets and rehypothecate them in an effort to earn yields that exceed the yields promised to their users. Although there is little public data as to the crypto lenders' investment strategies, anecdotal evidence suggests that the lenders employ a variety of strategies including secured lending, unsecured lending, "staking" in proof of stake cryptocurrency systems, and investing in equities.

Illustration 3: Repurchase transactions

118. A repurchase agreement (repo) facilitates short-term borrowing, primarily for dealers in government (Treasury) bonds. In a repo, a dealer sells government bonds, typically on an overnight basis, and buys them back for a slightly higher price. Government bonds may be swapped for a virtual currency, such as the JPM Coin that is a representation of the U.S. dollar held in an account of the participating bank. Repos may be conducted directly between the two parties, but also involve a third-party custodian.

Illustration 4: Purchasing cryptocurrencies on margin

119. 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 borrower will need to maintain sufficient collateral to cover maintenance margin requirements and top up the collateral if the Bitcoin value reduces.

Illustration 5: Central Bank Digital Currencies

120. 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/deposit based. It may require a supporting infrastructure where the CBDC, though issued by the central bank, is held by financial institutions for their customers. It may be used in a secured transaction either as original collateral or it may constitute proceeds of some other collateral. For instance, a financial institution that maintains a "CBDC account" for its customer extends a loan that is secured with the CBDC held in that account. A farmer may sell her crop in exchange for a CBDC that constitutes proceeds of the security right in the crop.

Illustration 6: Securing Exposures in Derivatives

121. A derivative is a contract the value of which is dependent on the value of another asset, such as a commodity. While it is possible to conclude derivative contracts with the underlying asset being a digital asset like a virtual currency, the focus is on the asset used to secure the respective obligations of parties to a derivative. Parties often agree to "put up" collateral to mitigate the risk embodied in their net exposure to each other. The most popular assets used as collateral in this context include cash, government bonds, corporate bonds, and equity. Collateral is usually provided in either of two ways: creating a security right or transferring title for the duration of the exposure. It is also common, and sometimes required, for the collateral to be held by a third party (custodian).

122. The potential use cases for digital assets in these transactions are only emerging. "Smart contracts", DLT and similar technology have already been deployed to automate various aspects of the transaction, including collateral management.[53] Regarding collateral, digital assets can play a role in two ways. Firstly, a digital asset with intrinsic value, like a virtual currency, can itself serve as the collateral. Secondly, a digital asset can be used as a token that has no intrinsic value but records or represents a "real-world" asset, which serves as the collateral.[54] Practically speaking, one of the main reasons why digital assets are not yet commonly used as collateral in this context is due to a lack of legal and regulatory certainty around their use, a lack of common documentation standards, and insufficient digitization and automation of collateral processes. In addition, the volatility of some digital assets specifically is likely to discourage their use within collateral management.

SECURED TRANSACTIONS PRINCIPLES - STRUCTURE

General notes:

- The process to develop one or more scope Principles for secured transactions may be different from the other SGs which start narrow and build from that base. Our working assumption is that all types of digital assets are covered, but some may need to be excluded based on different considerations. The exclusions may be of two types: 1) from the scope itself and 2) from the digital asset's specific rules. The consequence of the latter would be that the rules generally applicable to intangible assets will govern particular aspects of security rights in digital assets.
- States may 1) be satisfied that the existing law adequately supports the types of secured transactions commonly subject to that law; 2) amend their existing secured transactions laws, such as to include digital assets specific rules or 3) enact digital assets specific statutes. The latter may be appropriate particularly when a State enacts a comprehensive statute governing transactions with digital assets. In that case, the State will need to consider various forms of interaction with the general secured transactions rules, such as in the case 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.
- 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, or amenable to amendments.

---

[53] See International Swaps and Derivatives Association (ISDA) *Legal Guidelines for Smart Derivatives Contracts: Introduction* (Jan 2019) and ISDA *Legal Guidelines for Smart Derivatives Contracts: Collateral* (Sep 2019).

[54] See e.g., ISDA *Private International Law Aspects of Smart Derivatives Contracts Utilizing Distributed Ledger Technology: Japanese Law* (Oct 2020) 14-16.

- The secured transactions Principles may include a statement about a desirable general feature that the law should have (e.g., a security right may be created by an agreement without requiring an additional step, such as registration). Alternatively, the first Principle that generally recommends to States to create a clear and simple regime may be amplified to combine various general features of a modern secured transactions regime. The secured transactions Principles should not be limited to general statements about what the features the law should have without any reference to digital assets.
- The draft Principles may combine various elements relevant to the same aspect of a secured transaction (e.g., the principle on "creation" may address the issue of the ability to secure any obligations with any type of movable asset, as well as their description in a security agreement). If the individual elements are deemed critical to enable a particular transaction, they may be separated out into a specific Principle.
- The secured transactions regime may allow the parties to opt into its rules or opt out of it. The latter is generally limited by identifying the rules that are not subject to party autonomy, particularly those that affect third parties (e.g., on perfection and priority). While an opt-in to a regime should be generally facilitated as it is likely to increase legal certainty, any attempts of parties to collateral transactions involving digital assets to exclude the application of that regime would be limited by the mandatory rules. For instance, the application of a particular regime may be conditioned on the satisfaction of some functional criteria, such as the capability of being credited to a securities account and disposal by a credit and debit. See Art. 1(a) of the Geneva Securities Convention for inspiration.
- The following is an exhaustive list of issues that serves as guidance to the discussion of the secured transactions Principles. The intention is not to provide a principle for every individual aspect.

Specific issues for consideration:

Scope

A. DAs that
    a. have an obligor/issuer and
    b. those that do not.

This distinction is relevant in a number of aspects, such as perfection [what actions an intermediary or issuer might need to take] and enforcement [should one be able to enforce extra-judicially against a custodian when perfected by registration].

B. Possible exclusions – [for guidance and inspiration, see Article 1(3) of the UNCITRAL STL Model Law]
    a. One type of exclusion concerns the use of DAs as collateral in financial transactions, such as derivatives. The project may take a broader view, but invite States to consider whether some exclusions are appropriate, referencing the work of ISDA. In any case, the project should not attempt to formulate Principles for every plausible transaction.
    b. The scope discussion should take into account the Geneva Securities Convention regarding digital assets that may be treated as intermediated securities. Following the UNCITRAL Model Law's scope provisions might be too limiting.

C. Consumer protection statutes and regulations will continue to apply, but the Principles shall not deal with those (the Issues Paper highlights the focus on commercial transactions and trade). It would not be necessary to formulate principles concerning

secured transactions affecting consumer issues. The project should assume that other generally applicable legislation, including on consumer protection continues to apply.

Creation [See draft Principle D below]

A. How to enable persons to use their DAs as collateral?
    a. A power to transfer control, rather than demonstrating some property right should suffice (see Art. 6(1) of the UNCITRAL STL Model Law)
    b. Generic descriptions of the collateral and future property
    c. The notion of proceeds – scope, creation, perfection

Perfection

A. Confirm that registration achieves third-party effectiveness (perfection) with respect to all types of DAs (see Art. 18(1) of the UNCITRAL STL Model Law)
    a. No need to suggest that a State must establish a registry if it has not done so, as this is not a general secured transactions project. Where applicable, the State should ensure that the existing mechanism that is available to perfect a security right in intangible assets is equally available for security rights in digital assets.
    b. No need for the Principle to require a specific type of registration (e.g., notice-based) that is considered more efficient.

B. Should the Principles provide for specific perfection mechanisms?
    a. Control (see Art. 11 of the UNCITRAL Model Law on Electronic Transferable Records for inspiration)
        i. Direct by the secured creditor and constructive (e.g., through a custodian)
        ii. Technical Multiple signature arrangements
        iii. Should control be considered for the individual types of DAs from the taxonomy or generically?
        iv. Given the nature of this instrument as high-level Principles, should a Principle set out some parameters of control (e.g., exclusivity of certain powers)? [SG3 should simply consider whether the control parameters for perfection may need to be different from transfer, and, if not, defer to SG2]
    b. "Designating entry" for those DAs that have an issuer. See Art. 27 of the UNCITRAL STL Model Law and Art. 12(3) of the Geneva Securities Convention for inspiration.

Priority

A. Conflicts between secured creditors
    a. Perfected by the same method (temporal rule)
    b. Perfected by different methods (non-temporal rule) [Control may be considered a stronger perfection method, at least for those DAs that are of the virtual currency variety, but it may not be an appropriate approach for those that are more like general intangibles or tethered. Digital twins (i.e., DAs which are tethered or linked with real-world assets) will be subject to further discussions at a later stage.]

B. Rights of transferees
    a. The rules on transfers and innocent acquisition are a precursor to a number of aspects – [consider the work of SG2 on this aspect]

C. Conflicts with non-consensual claims
    a. Effectiveness of a security right in insolvency [Restate in a Principle that a properly perfected security right is effective in insolvency, and for any remaining

aspect coordinate with SG1 on the insolvency of custodians. See Art. 12(2) of the Geneva Securities Convention for inspiration.

b. Priority against "lien creditors" (e.g., judgment creditors) outside of insolvency [A Principle won't cover how one becomes a lien creditor with respect to a DA, and only limit itself to the priority aspect].

D. Conflicts between transferees of DAs and transferees/holders of tethered assets [This aspect may not even need to be dealt with depending on the direction of the project overall i.e., whether such DAs would be covered by the Principles].

Rights and obligations of obligors, custodians and issuers

A. What should be the rights and obligations of obligors towards secured creditors? [analogy to debtors of receivables].

B. What should be the rights and obligations of custodians that hold DAs subject to a security right [analogy to securities intermediaries]

C. What should be the rights and obligations of issuers of DAs with respect to any DA as well as a "real-world" asset that is tethered to the DA? [analogy to issuers of warehouse receipts].

A single Principle may cover all of these situations stating that these third parties do not owe any duties to the secured creditor unless they have otherwise agreed. This Principle may also cover some conflict of laws aspects, especially that their rights and duties vis-à-vis secured creditors are governed by the law applicable to their right and duties vis-à-vis the grantor.

Enforcement

A. A Principle should consider what rules are necessary to enable enforcement of security rights in DAs that also provide adequate protection to affected parties, such as competing claimants. While the general obligation to proceed in a commercially reasonable manner should continue, certain exceptions from otherwise applicable rules may need to be considered, such as to notify third parties entitled to receive a notification under the general secured transactions law of any disposition of a DA upon default.

B. Depending on the scope of the Project, close-out netting may need to be expressly recognized. A Principle may need to simply provide that any remedies already recognized by the domestic law should, with some appropriate adaptations, apply to security rights in digital assets. See Art. 71(1) of the UNCITRAL Model Law for inspiration.

Conflict of laws/private international law

A. SG4 discussions are a precursor. The law governing third-party effect of a transfer may be applicable also to the perfection and priority of a security right.

B. New perfection methods, such as control may necessitate new connecting factors, including for the perfection of a security right.

Principle A: Secured transaction law applies to digital assets

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

Comments. 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 collateral 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 "collateral transactions" should be understood to include various types of "security rights", such as pledges, charges, or security assignments, but also outright transfers where those might be used with respect to certain types of digital assets, such as those that are functional equivalents of securities or 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. The UNCITRAL Model Law applies to outright transfers of receivables. 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. The law governing collateral transactions must be coordinated with the generally applicable rules governing outright transfers of digital assets.

Illustrations:

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 custodian. It is unclear whether the account that holds the CBDC is a bank account that falls within a definition provided in the applicable secured transactions law.

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 unclear whether the court would recognize that delivery of the hard drive with access credentials constitutes a traditional possessory pledge that has been applied to tangible assets only.

Notes. Domestic laws may recognize a single (unitary concept) or multiple security devices that may be used in collateral transactions. Some of those may have limitations that would exclude the use of digital assets, while some are sufficiently broad to enable the use of any intangible assets. Many existing devices are antiquated so a legislative action to clarify their application to digital assets might produce sufficient certainty.[55]

The relevant secured transactions regime may not have a universally recognized 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 in most States, intangibles, other than embodied in a negotiable document of title, instrument or security, may not be pledged.[56] In other States, it is unclear whether the courts would recognize some form of delivery of a digital asset as a functional equivalent to delivering a tangible object to create a pledge. Yet, in another group of States, the pledge may extend to intangible assets that is effectuated by assignment in security.[57]

[55] 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.

[56] 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.

[57] 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.

Principle B: Digital assets are eligible to be collateral

The law should make it possible to use any digital assets as collateral. References in laws to movable assets, personal property or any similar notion for security purposes should be understood to include digital assets, regardless of whether digital assets are characterized as property or subject to a property right in that jurisdiction.

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 enables prospective secured creditors to decide for themselves which of the digital assets of a loan applicant have any collateral value.

Illustrations:

A secured creditor takes a security transfer of ownership of a digital asset. The rules governing this security device presuppose that the borrower owns the asset. Given that limitation, it is unclear whether the security transfer of ownership is perfected since the borrower may not have any recognizable ownership right in the first place.

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.

Notes. A secured transactions regime may define a security right as a "property right in a movable asset", without defining "movable asset".[58] On the one hand, persons may grant interests in any of their assets, whatever their nature, tangible or intangible, and present or future. This is contrary to some laws which are rather restrictive and enumerate the specific types of assets that can be encumbered. Such an approach might require amending that law to allow for the use of digital assets as collateral. On the other hand, the notions of movable property, personal property, things, or objects that may be subject to a security right are typically left undefined by secured transactions regimes, which creates uncertainty as to whether these notions cover digital assets. A security right may not be statutorily defined, but rather be generally understood in case-law and literature as signifying a right over property.[59] Under these regimes, a security right can be taken over any kind of property, tangible or intangible, present or future; anything that is transferable and identifiable.

Some laws allow the creation of an interest with respect to anything that can be traded, including intangible assets.[60] 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 provide greater legal certainty.

[58] 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)).

[59] 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.

[60] 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.

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

The law should recognize control as a mechanism to achieve third-party effectiveness of a security right. The law should recognize various forms of control that reflect the manner in which the digital asset is held and the type of creditor that extends credit on the security of the digital asset, including by acquiring exclusive powers over the digital asset. The law should specify which (if any) of its existing control 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 provide a public notice of the 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 are inapplicable to digital assets (e.g., delivery of possession of a tangible object) while others apply only to designated 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 to make the security right/pledge effective against third parties.

While in some States registration may be a mechanism generally available to render a security right effective against third parties with respect to any assets, registrations are not commonly effectuated in the crypto-lending market. However, 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 that recognize security rights as effective against third parties without taking any step beyond executing a transfer agreement, a transfer to a wallet should be sufficient to protect the security right against third-party claims, including in insolvency. For instance, a security transfer of ownership or an assignment for security purposes over financial instruments may not require any formalities. Digital assets that qualify as financial instruments may be assigned for security purposes with the right of the creditor effective against third parties without having to provide some form of public notice. In contrast, in other regimes the failure to register a notice may be fatal for the secured creditor, as no other mechanism would be applicable to achieve third-party effectiveness of a security right in a digital asset.

Secured transactions and related laws may already provide for control over an asset that may effectuate its transfer, whether outright or in security. The requirements to establish control may vary, including i) execution of a control agreement if the relevant asset is held with an intermediary (e.g., 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). In the past, regimes governing security rights in certain types of assets have been amended recognizing the industry practice (e.g., book entries to securities accounts in which financial collateral is held) where "the financial collateral is delivered, transferred, held, registered or otherwise designated so as to be in the possession or under the control of the secured creditor". Where laws 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. In any case, States may wish to include a specific definition of control to achieve third-party effectiveness conditioned on the secured creditor acquiring a set of powers (see Principle X) and adapt the definition of "control agreement" in the Geneva Securities Convention to the holding of digital assets with custodians.

This project has developed Principle X on control that is suitable to achieve third-party effectiveness of security rights over a broad range of digital assets by transferring the powers specified therein to the secured creditor. In addition, this project has developed Principle Y dealing with custody of digital assets. If a person that qualifies as custodian undertakes to follow instructions of the secured creditor in a control agreement the secured creditor would acquire

control. Incorporation of one or more of these control mechanisms into the secured transactions law affects the structure of its priority rules, which is explored below in Principle G on priority of security rights made effective against third parties by control.

The criteria that establish control under Principle X are also suitable for third-party effectiveness of security rights over intangible assets that might not be digital assets of the nature covered by this project, particularly "electronic transferable records" covered by the UNCITRAL Model Law on Electronic Transferable Records. This Model Law 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 to achieve third-party effectiveness of a security right.

Illustration:

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.

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

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. Separation of digital assets from the general category of intangible assets would enable the State to consider whether specific approaches, such as the perfection by control are necessary to reflect the prevailing practices.

Comments:

If digital assets are property, movable assets or a similar notion, they may fall under different types of collateral defined in the secured transactions regime. 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 a specific nature of the asset or the structure of the system in which it is transacted in mind, which could cause challenges in determining how those rules are to be applied to security rights in digital assets. A single digital assets type that covers variations of digital assets with different features or multiple characteristics may be provided for. 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 be impractical. 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". A State should coordinate the classification of digital assets with those for the purpose of other laws, particularly to enable the application a common set of rules, such as on control.

Illustrations:

The secured transactions law does not carve out digital assets from the broader type of intangible assets. Control 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, even though it might have effectively acquired control of the digital asset used as collateral. 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 (E): Insolvency law should recognize the third-party effectiveness and priority of security rights established prior to the opening of insolvency proceedings

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 creditors in any insolvency proceeding.
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.
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.[61] 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.

The degree of protection during insolvency proceedings may also depend on whether the digital asset qualifies as "cash proceeds". Cash proceeds may be used by the insolvency administrator only subject to providing adequate protection to the secured creditor. [see below a question to the Working Group].

Determining whether, and to what extent, a secured creditor is actually secured and may claim the value of its security interest, 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 to facilitate 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.

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

[61] The insolvency proceedings include collective proceedings in the form of reorganisation or liquidation.

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 for the Working Group:

- The aspects of third-party effectiveness and priority are covered by the UNCITRAL Model Law, so this Principle first reiterates that the relevant article of the Model Law would apply to security rights in digital assets. Is this redundant?
- There are some other aspects of insolvency directly related to security rights, such as the treatment of proceeds. Should this Principle expand on those?
- Several issues arose in connection with valuation of digital assets in insolvency. If this aspect is within the scope of the project, should this principle be expanded to deal with valuation?
- How should some other insolvency aspects, such as the insolvency of a custodian and the law applicable to insolvency proceedings be coordinated?

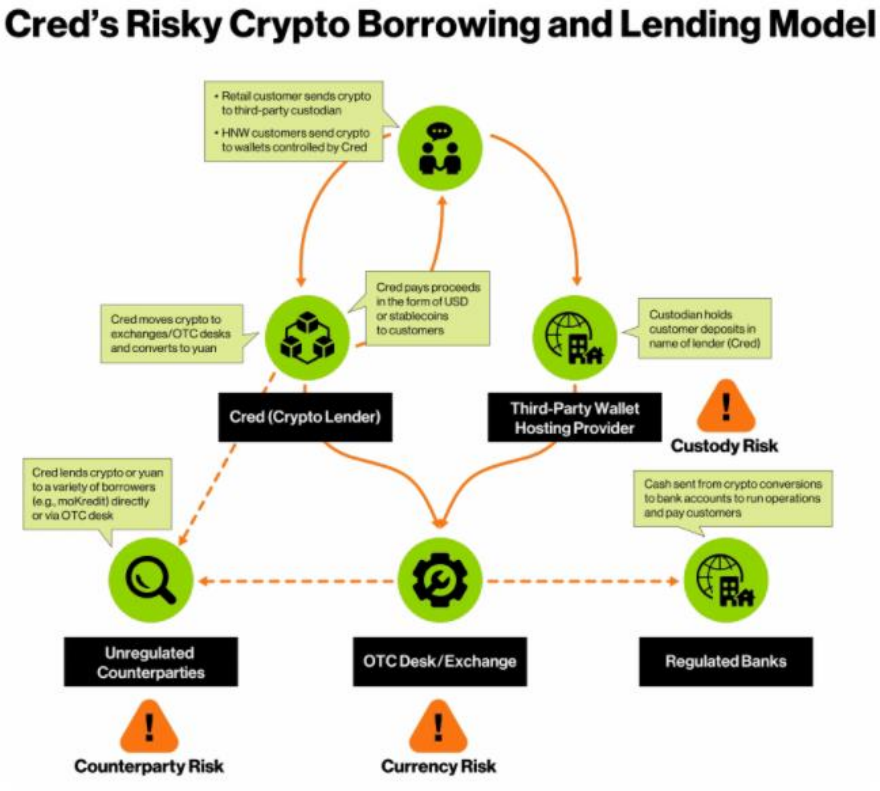
Cred bankruptcy case

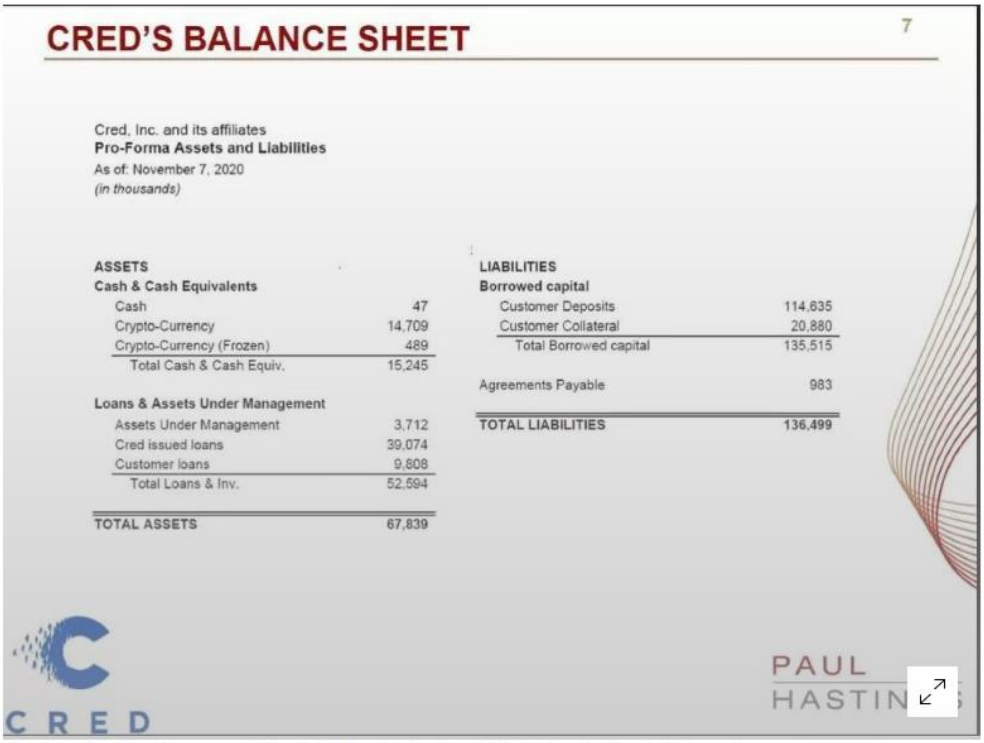
The case regards Cred Inc., a centralized cryptocurrency lender that filed for bankruptcy in November 2020 (US Bankruptcy Court for the District of Delaware). Cred is a cryptocurrency investment platform, describing itself as a "global financial services platform" and "licensed lender" that delivers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

7

Cred, Inc. and its affiliates
Pro-Forma Assets and Liabilities
As of: November 7, 2020
(in thousands)

ASSETS	
Cash & Cash Equivalents	
Cash	47
Crypto-Currency	14,709
Crypto-Currency (Frozen)	489
Total Cash & Cash Equiv.	15,245
Loans & Assets Under Management	
Assets Under Management	3,712
Cred issued loans	39,074
Customer loans	9,808
Total Loans & Inv.	52,594
TOTAL ASSETS	67,839

LIABILITIES	
Borrowed capital	
Customer Deposits	114,635
Customer Collateral	20,880
Total Borrowed capital	135,515
Agreements Payable	983
TOTAL LIABILITIES	136,499

CRED

PAUL HASTINGS

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)[62], 2) Pledge agreement.[63]
- 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."[64] Of Cred's $136 million in liabilities, $114 million is owed to holders of Cred Earn notes.[65] 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…".[66]

Principle X: Priority of security rights in digital assets made effective by control

The law should recognize that where a security right in a digital asset has obtained third-party effectiveness through control under Principle Y, the security right should have priority over a security right in the digital asset of a person who does not have control. 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 or a security right **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, money, negotiable documents**, and other types of assets**. Providing for this non-temporal priority recognizes that the secured creditor that took the additional steps was relying to a greater extent on the encumbered asset.

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

---

62 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

63 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."

64 p. 15 of the Liquidation Plan (21.01.2021).

65 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.

66 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.

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 its security right in the registry or otherwise made it effective against third parties. If it is possible under Principle Y that more than one secured creditor can obtain control (or share such ability) over the digital assets to make their security right effective against third parties, there should be a rule to determine the priority between the two secured creditors based on the temporal order of obtaining control.

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

123. 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.

124. Given that the private law treatment of digital assets as property may affect whether digital assets belong to a debtor's insolvency estate[67], 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.

125. 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.

126. 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.

6. Remedies and Enforcement

127. 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

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

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.

128. 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.

129. 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.[68] 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.

130. 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

131. 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 other organisations[69] 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.

132. At its second session, the Working Group agreed on three issues to be addressed by the tentative Principles: (i) the law applicable inside the digital assets platform (network)[70] 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

---

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

[69] 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.

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

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.

PIL – 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?

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 June 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)

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*)	PhD candidate Université de Genève Switzerland
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

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 (CET)

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

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 Carlton Fields United States of America
AMERICAN LAW INSTITUTE (ALI) *(Observer)*	Mr Steven WEISE Partner 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 (CET)

SG3 – Fifth Meeting – 11 June 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 Carlton Fields United States of America

EUROPEAN BANKING INSTITUTE (EBI) (*Observer*)	Mr Matthias LEHMANN Professor Universität Wien EBI Germany

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)

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
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

ANNEX III

COMPARATIVE RESEARCH TABLE

(FOR INTERNAL USE ONLY – NOT FOR CIRCULATION)