



EN

**Digital Assets and Private Law
Working Group**

Second session (remote)
Rome, 16 – 18 March 2021

UNIDROIT 2021
Study LXXXII – W.G.2 – Doc. 2
(rev. 1)
English only
March 2021

ISSUES PAPER

1. This document provides a discussion of issues that the Digital Assets and Private Law Working Group may wish to consider 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)
 - (v) Participants in Sub-Groups as part of intersessional work conducted between January and March 2021
 - (vi) The Chair of the Working Group, or
 - (vii) The Secretariat

The document is not intended to provide an exhaustive list of issues nor a full legal analysis of each issue. The purpose of the document is to provide a starting point for the Working Group's deliberations and a structure for discussions at the second meeting.

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

4. The document contains an annex that provides links to relevant documents to assist the Working Group (**Annex I**) as well as an annex providing the full list of participants in the Sub-Groups set up to carry out intersessional work (**Annex II with Appendices**).

TABLE OF CONTENTS

I.	PRELIMINARY MATTERS	3
	A. Background	3
	B. Format of the Guidance Document	5
	C. Target Audience	5
	D. Title of the instrument	6
	E. Terminology	6
	F. Composition of the Working Group	6
	G. Methodology and Organisation	7
	H. Establishment of a Steering Committee	8
II.	SCOPE OF THE GUIDANCE DOCUMENT	8
	A. Relationship with existing instruments and other projects of the current Work Programme	8
	B. General: Private law relating to Digital Assets, in particular proprietary interests	9
	C. The subject matter of the project	9
	D. Identify specific areas/issues of private law to be addressed	15
	1. Issues relating to the contract involving digital assets	15
	2. Acquisition, disposition, and competing claims	16
	3. The legal nature of a proprietary connection between digital data and another asset	20
	4. Accommodation of disparate types of assets and technologies	21
	5. Provision of digital asset custody services	21
	6. Taking of security over digital assets	24
	7. The legal treatment of digital assets in relation to insolvency proceedings	36
	8. Remedies and Enforcement	36
	9. Law applicable to issues relating to digital assets	37
	Annex I – ADDITIONAL RESOURCES	40
	Annex II – INTERSESSIONAL WORK	43

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” (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).

10. The Governing Council recommended to the General Assembly that it include this item at medium priority on the 2020-2022 Work Programme ([C.D. \(98\) 17](#), para. 275). The General

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>.

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) which set out the Secretariat’s proposal on the most appropriate scope for this project, considering that further refinements should be entrusted to the experts who will be selected as members of the Working Group for the project.

13. In broad contours, the proposal described a project that would aim to do the following:

- “The project would develop Principles relating to the legal nature, transfer and use of tokens. It would focus on private law, and not regulation. It would consist of a legal taxonomy, and consideration of issues arising in various important contexts, such as insolvency, secured transactions, identification of the applicable law in cross-border transactions, and the legal position of intermediaries involved in the token markets, such as exchanges and custodians.
- It would take a functional approach, neutral as to legal culture. It would therefore seek to identify the rights and obligations arising, without giving bundles of rights and obligations labels, such as ‘property’, which vary amongst jurisdictions.
- It would be necessary to consider how far the Principles developed by the project are consistent with existing law. Despite the fact that tokens are a ‘new’ type of asset, consistency with legal treatment of other types of asset could be seen as important, and consideration will need to be given to what extent existing legal Principles can apply by analogy, and what modifications are required.
- The project would also take a neutral approach, as far as possible, in relation to technology, so as to ‘future proof’ the Principles. In other words, it would seek to develop Principles that could apply to any system in which data could constitute a token (that is, an asset which could only be spent once), rather than being specifically applicable to systems based on DLT or blockchain. In this way, the danger that the work would be overtaken by technological or market developments would be minimised”.

14. On the basis of feedback received from the Governing Council at its 99th session (A) the Secretariat prepared an amended proposed action, namely:

- “to begin work on the project (i) remotely, in order to avoid costs, and (ii) limited to further refining the scope of the project.
- In order to conduct this limited work until the second meeting of this session of the Governing Council in September, the Secretariat requested authorisation to select a limited group of experts, which would naturally evolve into the core of the future Working Group. This core group would assist the Secretariat in the preparation of a more developed

document for the September meeting. In addition to incorporating comments and analysing topics arisen as a consequence of this discussion, said document would include (i) details of the full Working Group, (ii) a detailed timeline of a proposed action plan, and (iii) an explanation as to how this project would feed into – and hence create synergies – with other projects of the current Work Programme.”

- To change the name of the project to one that better represented the content of the work.

15. The Governing Council agreed to approve the scope and upgrade the level of priority, as well as to follow the amended proposed action by the Secretariat ([C.D. \(99\) A.8](#), paras. 57-58).

16. 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.

17. 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.

18. 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

19. 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 would 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.

20. 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

21. 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

22. 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

23. 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

24. Existing instruments use different terminology for related concepts. The Working Group 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

25. 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.

26. 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)

27. 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 (IVASS)

28. 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

29. 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.

30. 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 (likely remote)
 - Fourth session: Last quarter of 2021 (tentatively November 2021)

- 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

31. 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.

32. 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

33. 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.

34. 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).

35. 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.

36. 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.

37. 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

38. 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.

39. 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 appropriate and where considered to be 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.

40. 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

41. The project is concerned with assets that are constituted of digital data which has certain features, including that it is amenable to control (in the functional sense), as described in the

paragraphs below. At its first session, there was consensus amongst the Working Group that an iterative approach would be desirable, allowing for the discussion of scope to be continuously refined as discussions of the more substantive issues advance and help in further defining the broad contours of the project. This is therefore an issue which will need to be kept under constant review throughout the deliberations of the Working Group. Accordingly, this section of the issues paper sets out some preliminary guidelines rather than precise definitions.

42. The project is not concerned with all types of digital data. As explained below, not all digital data can be characterised as an “asset”, and there are even some types that could plausibly be considered as an “asset” which the Working Group may wish to exclude from the scope of the project. Indeed, at its first session, the WG agreed that certain kinds of digital data which have an economic value ought to be excluded from the scope (e.g., browser history, digital images, etc.)

43. While the term “asset” can have many different meanings, it is used here in the sense of an object which has value ascribed to it; that is, people are prepared to transfer other objects of value (such as fiat currency) in order to acquire it. Such objects exist within systems that comprise hardware, software, and personal and community aspects, although the social structures and roles implicated in the process may not be well-defined and are sometimes obscured by claims that a system is purely technical, leading to an exclusive focus on its digital components.

44. The focus of the project is on private law, and, in this context, this implies, generally though not exclusively, property law (widely construed). Therefore, in the first instance, this project is concerned with digital assets that are plausibly *objects of property rights*, or perhaps rights similar to property rights. The focus on proprietary rights, however, presents a difficulty in terms of distinguishing cause and effect. Current principles of property law in different jurisdictions yield contradictory answers to the question whether any particular type of electronic data can be the object of proprietary rights, and indeed suggest quite different approaches to conceptualising intangible representations of value generally. Not all types of electronic data that the project will examine are considered as “property” in some jurisdictions.⁴

45. The Working Group considered during its first session the possibility of conducting a brief survey regarding the variety of approaches relating to the “property status” of electronic data typically found across national jurisdictions and the consensus was that any survey ought to wait for the work to commence and identify specific issues for targeted surveys to be subsequently conducted (if and as needed). The Secretariat has begun collecting the existing surveys out there at this stage and the relevant references are included in the corresponding footnote as well as in **Annex I**.⁵

46. There was consensus amongst the Working Group that it was necessary to take a broader view of the subject matter to define the scope of this project, whose purpose was to develop a set of Principles, at the transnational level, that courts and legislatures can use to guide legal interpretation and reform. The Working Group agreed that work could begin by considering some examples of existing types of digital data to assist with the task of more clearly delineating the scope

⁴ In Japan, the Tokyo District Court confirmed in a 2015 decision in the *MtGox* case that Bitcoin could not be classified as a “thing” for the purposes of the property law regime under the Civil Code of Japan (Tokyo District Court, *Plaintiff Z1 v. MtGox Co. Ltd.*, Case No. 33320 of 2014, Judgment, 5 August 2015) (<https://www.law.ox.ac.uk/research-subject-groups/commercial-law-centre/blog/2019/02/english-translation-mt-gox-judgment-legal>). In Germany, the government has released a draft bill which proposes to deem electronic securities without a paper certificate as objects of property pursuant to art. 90 of the BGB. (https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/RefE_Einfuehrung_elektr_Wertpapier_e.pdf?__blob=publicationFile&v=1).

⁵ Following input from the WG participants, a number of existing surveys were collected, notably the following: Global Standards Mapping Initiative (GSMI) Report (2020), <https://gbbcouncil.org/wp-content/uploads/2020/10/GSMI-Legal-Regulatory-Report.pdf>; Stanford Law School’s CodeXRegTrax, The Stanford Center for Legal Informatics, <https://law.stanford.edu/codex-the-stanford-center-for-legal-informatics/regtrax/>; and CoinLaw, mobile app available from the law firm Perkins Coie, <https://appadvice.com/app/perkins-coie-coinlaw/895563535>.

of the study. This might include, first and foremost, cryptocurrencies (e.g., Bitcoin) and digital assets that in some fashion represent, are backed up by, or are linked to other assets (e.g., commodities).

47. The Working Group further affirmed that the principle of technology neutrality was also important in scope-setting and while DLT or blockchain technologies would constitute an important facet of the project's scope, the Working Group should not consider itself restricted to any one specific technology in seeking to identify and articulate Principles. It was agreed that the scope needed to be broader than just the category of cryptoassets.

48. As mentioned in D.3 below, it is possible to analyse the DLT-based digital data alternatively as (a) a record of the transfer of an asset, or (b) as a separate asset in its own right. Whether this analysis is a suitable one, in what situations it applies and the legal ramifications of this analysis are all issues the project will have to consider. For present purposes, the term "digital assets" is used to include DLT-based digital data that has the factual features set out below, even though the term "assets" may be thought wrong or misleading. The distinction between DLT-based digital data that does not relate to an asset that exists irrespective of that data, and DLT-based digital data that does relate to such an asset is a very difficult one.

49. This distinction is a matter which the Working Group will discuss under D.3 as it concerns the taxonomy of digital assets rather than the scope of the project, in the sense that the question whether in any particular situation the DLT record is evidence of ownership of an off-chain asset or whether it constitutes an asset in its own right is a matter for the Working Group to continue to discuss.

50. The question then arises: What are the *factual features* which distinguish those digital objects that should be recognised as objects of proprietary rights from those which should not? In this context, a functional approach could be called for, and the object's amenability to *control* would seem of paramount importance. In previous work on the harmonisation of private law (for example the UNCITRAL Model Law on Electronic Transferable Records) the concept of control has been adopted as an analogue of possession, given that electronic records are not capable of possession in the ordinary legal sense, which implies amenability to *physical* possession in the factual sense. When defining the scope of the project, given that different jurisdictions have different legal definitions of control (indeed, sometimes the same jurisdiction uses 'control' to mean different things in different contexts) a legal concept of control may not be appropriate as a scope defining criterion, even if a particular definition of control could be adopted later on in recommendations as a requirement, for example, for a person to be a holder of a digital asset or for the application of an exception to the *nemo dat* principle. During its first session, the Working Group noted that while the notion of control could present some challenges, it was agreed that the concept was clear enough in a broad sense that it did not need to be defined specifically before the Group could proceed with its work.

51. Other features may be of relevance to distinguishing categories of electronic data which fall within the scope of the project from those which do not. For example, the question whether a unit of data can be individuated from a broader volume of data might be significant, as might the question whether the "package" of data in question can be copied infinitely or is somehow protected from replication at will, or the question whether the data can be treated as an object of value by more than one person at a time (without any derogation of the others' ability to use it) (e.g., a digital representation of a song or a piece of art).⁶ These features run together; for example, a unit of electronic data could be said to be rivalrous because it cannot be copied infinitely at will and because it can be individuated from a broader mass of electronic data. This relates to the deeper question of what kinds of electronic data should be considered "assets" at all. In summary, digital assets are a

⁶ This feature does not exclude the possibility that a given asset might be owned jointly by multiple parties, or that its owner might grant e.g., use rights or securities rights to others; rather, it has to do with the preliminary question whether it is a fitting object of property rights in the first place.

subset of all types of electronic data, and the scope of the project relates to a subset of “digital assets”.

52. In its discussions at its first session, consensus emerged within the Working Group that the focus of the project was on those categories of digital data which: (i) had an economic value, (ii) were the object of exclusive control, and – where that caused legal issues (iii) were transferable (transferability or tradability being understood as functional notions rather than legal ones). Consensus also emerged around the following points concerning definition of subject matter:

- that a descriptive, neutral approach to scope is preferable;
- that it would be premature to use concepts and terms such as “transferability” and “control” in terms of setting the scope, especially given that terms like transferability lack international consistency in their use, although it was agreed that transferability may be helpful in the functional sense;
- that analytical work would need to be carried out to further refine the scope. Accordingly, rather than get attached to terms which presupposed certain definitions, the WG should focus on a factual description of very practical cases it wished to examine;
- it was further agreed that certain kinds of digital data which have an economic value ought to be excluded from the scope (e.g., browser history, digital images, etc.).

53. At its first session the Working Group agreed that work towards creating a taxonomy of digital assets for private law purposes could bring value and should be part of the Project. More specifically, the WG agreed that such a taxonomy should have the following features:

- be focused on private law issues aimed at a legal audience such as legal practitioners, judiciary, and legislators (as opposed to a regulatory or technical audience);
- be tied closely to the Principles, rather than seeking to create definitions just for the sake of doing so;
- the taxonomy work should seek to illuminate the legal concepts and relationships between legal concepts.
- Further, in terms of the sequencing, it was the WG’s view that the first step would be mapping out the relevant legal concepts, and then the definitions could be more specifically defined as the work on the Principles had progressed.

54. 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**).

55. The Working Group is invited to consider and discuss the paper describing the initial scope of the taxonomy work stream which was prepared by the co-chairs of Sub-Group 4 following discussions within the Sub-Group.

Note on Taxonomy (SG4)

Context

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

57. The taxonomy will inform and accompany this work. 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 protocol⁷ (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.

58. 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 terminology used by other work streams and ensure that the definitions are consistent with the taxonomy and coordinated.

59. The taxonomy is likely to be an iterative process throughout the course of the Project.

Overarching principles

60. In so far as possible the taxonomy should be technology neutral and future-proof.

Scope – 'digital asset'

61. As was expressly stated by the Working Group during the first session, the intention is to start broad. At this stage there is agreement for the Sub-Group not to limit itself even to 'crypto-assets' as it is not yet clear that the use of cryptography should be a characteristic delineating what is in or out of scope of the Project's work.

62. Additionally, it has been agreed that the mode of issuance or type of issuer (private or public e.g., central bank) should not be considered a delineating feature at this stage. Nor should regulatory classification (e.g., 'financial instrument' under MiFID or 'security'), 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).

63. However, it is recalled that here we are not referring to 'digital unit' (pure code), rather 'digital asset' - so 'asset' must have some significance.

64. Importantly, 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.

For these reasons, our **working approach is to define 'digital asset' as a:**

***digital [representation] of:
[a unit to which financial value is [attributed]],
[a right], or
[a claim]***

It remains open to discussion whether each of these elements needs to be reflected in the definition. It is easy to see that 'a unity to which financial value is attributed' is needed for something like Bitcoin (which has no underlying assets, no issuer, etc.) but it is more complex

⁷ For instance, a 'blockchain protocol' setting out a binding set of rules between the system participants in addition to the code that provides the technical functionality for the system.

where an asset confirms a right or claim – could this always be considered then an asset to which financial value is attributed (e.g., thinking of something like a utility token – some are tradeable, some are not)?

65. In view of the broad scope of the working definition, it should be noted that tokens such as gaming tokens, and perhaps even 'loyalty' points schemes and airmiles are likely to be in scope. As such, and depending on the overall scope of the Project's work, it is likely that some exclusions may be needed.

Sub-categorisation of 'digital asset'

66. The term 'digital asset' covers a vast range of cases – some where the value, rights or claims are limited to the purely digital sphere, and others where there is a whole or partial intersection with the 'real world' (this is a very shorthand expression to mean things that exist or are actionable 'off chain'). 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 'real world' asset as a matter of property law.

67. As such, one can anticipate already **several basic sub-categories of 'digital asset'** (*essentially building on 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 [digital representation] of a (i) moveable tangible, or (ii) immoveable tangible, or (iii) an intangible financial asset, or (iv) an intangible non-financial asset (e.g., IP).
[Definition of 'financial asset' to be considered by the Working Group.]
- **Category 2:** [The Sub-Group continues to consider whether we need a category 2?]
- **Category 3:** transferable code constituting a [digital representation] of a [unit] to which [financial value] is [attributed] but does not constitute a Category 1 asset (e.g., Bitcoin, Ethereum). [Here, there are no rights or claims against an issuer, nor any rights or claims in respect of any asset or person.]

68. 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).

Next steps: Questions for consideration

69. Sub-Group 4 welcomes reflections from the Working Group on the working definition of 'digital asset', including whether there is a need to include the three elements identified:

- rights;
- claims;
- value attributed to the unit (to account for cases such as Bitcoin the value for which is whatever someone wants to pay for it – essentially its intrinsic value)?

70. Sub-Group 4 welcomes the Working Group's reflections on the categories identified in paragraph 67, including any proposal for a definition of 'financial asset'. Working Group participants are invited to test the categories against observed examples of digital assets. Do the categories work? Do we need to sub-categorise any the categories, do we need to add any categories? Here we can recall some types of digital assets, including:

- digital representation of a *one-off right* (so-called 'utility tokens')
- Central Bank Digital Currencies

- fungible vs non-fungible tokens – is there a need to tease out any specific points in the context of the taxonomy?

71. By way of final remarks, Sub-Group 4 has discarded the consideration of so-called ‘stablecoins’ as a free-standing category. This is because 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):⁸

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.

72. 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;
- One can speculate as to lots of different scenarios e.g., at each extreme:
- (i) Token holders have a claim (under all circumstances) against the issuer in relation to the reserve.
 - (ii) Token holders have a claim against the issuer in relation to the reserve ONLY in the event certain events occur (e.g., full collapse of the system).
- [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).

73. Finally, Sub-Group 4 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 57, for instance factors ‘external’ to the assets themselves. This point will remain under review by the Sub-Group as the taxonomy work progresses.

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

1. Issues relating to the contract involving digital assets

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.⁹ Certain legal remedies in connection with the holding, transfer and collateralisation of digital assets may be attributed to contract law. For instance, in jurisdictions where digital assets are not characterised as property, remedies given to a customer against a custodian may be recognised in contract law.

⁸ <https://www.fsb.org/wp-content/uploads/P131020-3.pdf>.

⁹ For a representative and comprehensive study, see the ALI/ELI Principles for a Data Economy at <https://www.ali.org/projects/show/data-economy/>.

75. At its first session, the Working Group agreed that the project would consider contracts, but not through a contract law perspective (i.e., classic “pure” contractual questions such as ascertaining the enforceability of a given contract), but rather as the object of study (i.e., looking at what was expected to be found in a contract of transfer to effect a transfer, or to effect a property interest). It was noted that contractual issues could be identified in a number of other areas of the project, for example, in the examination of the minimum content of a custodian contract. Accordingly, it was agreed that the project ought to deal with contractual rules and issues wherever appropriate rather than define contractual issues narrowly.

2. Acquisition, disposition, and competing claims

76. Common law and civil law systems emphasise the role of *nemo dat quod non habet* (one cannot give what one does not have) in the transfer and acquisition of property interests. Civil law generally limits recognition and transfer of ownership, including exceptions from the *nemo dat* principle, to tangible property.

77. Once the law recognises a proprietary interest in an asset it should logically provide some protection to transferees. Acquisition of proprietary rights in digital assets may be by original acquisition (issue) or by derivative acquisition upon disposition. The analysis will consider basic, fundamental, building-block rules drawn from analogous rules applicable to the transfer, assignment, and acquisition of movables and intangibles generally. This sub-section addresses only the law governing acquisitions of digital assets in voluntary transactions occurring within a system, and thus does not cover transfers that may occur such as by way of succession or by operation of law pursuant to other laws or judicial process.

78. The application of property law rules generally depends on the identifiability of property and some form of publicity, as well as the following of transfers of interests in property from one person to another. The application of property rules also sometimes requires “tracing” of interests, which may require formulas or other methodologies. These concepts are particularly challenging in the context of digital assets. Moreover, some digital assets are fungible, and some are not. Ether and Bitcoin are fungible, for example. Non-fungible digital assets represent a unique asset that cannot readily be interchanged with other digital assets, even if two non-fungible digital assets seem similar to one another. Non-fungible digital assets can include metadata, visuals, serial numbers and other characteristics that make them unique, and, thus, uniquely valuable. Examples of a non-fungible digital asset would include unique digital items like crypto art, crypto-collectibles, and crypto-gaming tokens.

79. Digital assets commonly exist as part of, or as layered software on top of, an account-based system or a transaction-based system. Many existing and future designs (e.g., the central bank digital currency) contemplate one or the other, or both types. The Ethereum network, for example, uses an account-based model to memorialise which network users own any given quantity of ether. This makes ether transactions and the method by which the Ethereum network keeps track of those transactions much like the bank account model used by banks. One ether owner can simply send ether to another Ethereum user’s account, and the Ethereum Virtual Machine will track the transaction in those account balances.

80. Other digital assets effectively disappear upon transfer with new digital assets being created for the benefit of acquirers. In this regard, Bitcoin provides an example. The Bitcoin blockchain does not use an account-based model, but rather a transaction-based model. As a result, owners of Bitcoin do not lower a balance in an account they hold when they send Bitcoin to another user. Rather, the Bitcoin blockchain tracks transactions (or put differently, it tracks transitions in state). Take, for example, Alice. Colloquially, we might say that Alice “owns 25 Bitcoins”. But what Alice actually has is the key to unlock a single unspent transaction output (UTXO) that the Bitcoin blockchain associates with 25 Bitcoins. If Alice wants to send 17 of those 25 Bitcoins to Bob, she cannot split off part of

her single UTXO and send it to Bob while keeping the other eight in her “account.” Alice does not have an account. Alice must spend the whole 25 Bitcoins by creating two transactions: one transaction sending 17 Bitcoins to Bob, and one transaction of sending 8 Bitcoins to herself. As such, by unlocking her single UTXO and sending 17 Bitcoins to Bob, Alice creates two new UTXOs – one locking 17 Bitcoins to Bob and one locking 8 Bitcoins to Alice.

81. The acquisition of property free of conflicting claims is a feature of both common law and civil law systems, such as doctrines of good faith purchase or similar innocent acquisition rules. These are important exceptions to *nemo dat*. Some digital assets could be classified as a recognised asset type under existing laws, such as funds/money or negotiable instruments, for which existing take-free rules could be applied. Others would not fall under any existing specific type. Some digital assets are traded on platforms/exchanges while others in peer-to-peer markets.

82. Take-free rules and negotiability aspects of digital assets would require the adoption and application of relevant standards. Standards such as the absence of disqualifying knowledge or notice, good faith, and taking of possession (delivery) of tangible movables are typical. For digital assets, the standards would likely include the adoption of an equivalent to possession or delivery of tangible movables. A point of departure might be the approach toward “control” of electronic transferable intangibles developed in the UNCITRAL Model Law on Transferable Records and the various national laws from which the Model Law drew inspiration.

83. Digital assets may be subject to a wrongful taking or interference (such as by “hacking” in the case of digital assets held and accessed through the internet). The application to digital assets of legal doctrines of recovery and liability, such as common-law conversion or vindicatory enforcement of rights in civil law systems, will be considered. For example, conversion has been recognised by the courts in the United States with respect to intangible assets, such as domain names on satisfaction of certain conditions (that may be similar to recognising a digital asset as property): (i) there must be an “interest capable of precise definition”; (ii) it must be “capable of exclusive control”; and (iii) “the putative owner must have established a legitimate claim to exclusivity”.¹⁰

84. At its first session, the Working Group considered issues relating to the acquisition and disposition of and competing claims to digital assets, including in particular those that relate to proprietary (or analogous) interests in digital assets. There was agreement in the Working Group that addressing innocent acquisition rules and referring to invalidity and reversal in the Principles would be an important added value.

85. As part of the intersessional work that the Working Group agreed upon at its first session, Sub-Group 2 was established and led by co-chairs Matthias Haentjens and Charles Mooney, Jr. as they examined a range of issues relating to control and transfer of digital assets (a full list of the participants is available at **Annex 2, Appendix 2** along with a work program). The outcome of these meetings was the preparation of **two draft principles** together with a list of additional issues, found below, for the consideration of the Working Group.

¹⁰ It is noted here that the United States of America differs from English law and the common law of other jurisdictions as well.

**PRINCIPLE [X.1]
“Control”¹**

(1) The law of the [implementing] [adopting] State should [define] [specify the attributes of] the concept of “control” of a digital asset as the functional equivalent of possession of movables with adjustments to take account of the intangible nature of digital assets.

(2) In its [definition of] [specifications concerning] control an [implementing] [adopting] State should [consider including] [include] the following criteria:

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

(i) transfer control² of the digital asset to another person [(or the functional equivalent of a transfer of control, e.g., by replacing or modifying a digital asset and the resulting creation of a new digital asset controlled by another person)] ;

(ii) obtain substantially all the benefit from the digital asset; and

(iii) prevent others from obtaining substantially all of the benefit from the digital asset; and

(b) the digital asset or its associated records allows the person to identify itself as having the powers mentioned in (2)(a)[; and]

[(e) others].

(3) A power is exclusive for purposes of paragraph (2)(a) even if:

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

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

* * *

Questions for the Working Group / Additional issues to consider:

(i) Is the use of “exclusive” in (2)(a) confusing or misleading inasmuch as more than one person can share control? Would another term be preferable?

(ii) Is the language in square brackets in (2)(a)(i) necessary or is it sufficient that the concept is included in the Transfer Principles?

(iii) Should the identification mentioned in (2)(b) contemplate not only identification by the name of a person but by other means such as an identifying number, a cryptographic key, an office, or an account number?

(iv) Do these principles make it sufficiently clear that an unauthorized person (e.g., a “hacker” or wrongful acquirer of private keys) may obtain control or the power to transfer control? Should this be made explicit?

¹ 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.

² These draft principles assume that transfer of “control” is distinguished from a “transfer,” which contemplates the transfer of proprietary rights. A transfer of control may or may not be associated with a transfer of proprietary rights.

Figure 1: Principle X.1 on “Control”

**PRINCIPLE [X.2]
Acquisition and Disposition (“Transfer”) of Digital Assets**

(1) The law of the [implementing] [adopting] State should specify which (if any) of its rules or standards govern the acquisition and disposition of proprietary rights in digital assets.

(2) The law of the [implementing] [adopting] State should define the “transfer” of digital assets so as to include the disappearance, destruction, cancellation, or elimination of a digital asset and the resulting and corresponding derivative acquisition of other digital assets.

(3) The [implementing] [adopting] State should [consider whether and to what extent the law should address][specify] the legal consequences of a transfer of digital assets vis-à-vis the transferor and transferee *inter se* (such as *nemo dat non quod habet* or implied warranties of “title” or “quiet enjoyment”) or whether such matters should be left to [other] [the applicable] law.

(4) The law of the [implementing] [adopting] State should [address][specify] the legal consequences of a transfer of digital assets vis-à-vis third parties (i.e., “third-party effectiveness”).

(5) The law of the [implementing] [adopting] State should specify in particular the requirements for a transferee to qualify as an innocent acquirer of digital assets and the rights obtained by an innocent acquirer (e.g., good faith purchase, finality, and take-free rules).

(a) The State’s innocent acquisition rule should provide strong protection for innocent acquirers of digital assets to the end that innocent acquirers take digital assets free of conflicting claims (e.g., the attributes of negotiability).

(b) Concerning the test or standard for an acquirer’s protection under an innocent acquisition rule:

(i) The State should carefully consider whether to avoid use of the term “good faith” and similar terminology, taking into account the variety of meanings and interpretations under different legal traditions and the State’s own legal regime. It may wish to consider the use instead of more functional and objective factual standards.

(ii) The State may wish to consider 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.

(iii) The State should include an acquirer’s “control” of a digital asset as an essential element of the test or standard for innocent acquisition protection.

(c) The State should adopt (or retain or adapt) a “shelter” principle that would benefit onward direct and indirect transferees from an acquirer protected by the innocent acquisition rule. In other respects the rights of an acquirer that does not qualify for protection under the innocent acquisition rule should be specified by the State or left to [other] [the applicable] law (see (3) above).

* * *

Questions for the Working Group / Additional issues to consider:

(i) Should the principles propose a harmonized innocent acquisition rule?

(ii) Arguably implicit in the “control” element of an innocent acquisition rule is the protection of an innocent acquirer even if the transfer of control of the digital asset to the acquirer is wrongful (e.g., by a “hacker” or a wrongful acquirer of private keys having no proprietary rights in the digital asset). Should this be made explicit in the principles?

Figure 2: Principle X.2 on Acquisition and Disposition (“Transfer”) of Digital Assets

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

86. Some types of digital data (that has the features of individuation, control and being non-rivalrous) can be structured so as to represent other assets, in such a way that the holder of the digital data purports to have a proprietary right to that other asset.¹¹ The digital data in such a structure can be seen as a digital asset in its own right or can be seen merely as a digital record. The discussion in this paragraph assumes the former characterisation in order to make the terminology more straightforward. When the process of transfer of the digital asset takes place, the proprietary right to that other asset is transferred from A to B. One example is where a digital asset gives a right to physical goods such as gold (see e.g. <https://www.gcoin.com>) or art (see e.g. <https://en.cryptonomist.ch/2020/07/04/tokenized-art/>). Another example is where a digital asset represents a debt security, such as ‘tokenised’ corporate bonds (see e.g. <https://www.financemagnates.com/institutional-forex/exchanges/gibraltar-stock-exchange-to-offer-digital-debt-securities/>). The mechanism of linking one asset to another is sometimes called tokenisation, but what matters is the mechanism itself, and focusing on ‘tokens’ may be misleading in a proper legal analysis. The other asset will generally (but not necessarily) be an asset (tangible or intangible) that is not a digital asset. This type of digital asset is colloquially known by a number of different terms, including a “token” and a “coin”.¹²

87. Since it relates to proprietary rights, the legal analysis must consider the effect of such transfers on third parties. The legal analysis may vary depending on how the digital asset or data and the system on which it operates is structured, and so the Working Group may need to identify a number of possible analyses. The legal nature of this link may also affect the analysis of issues (II.D) 2, 6, 7, 8 and 9.

88. To give an indication of the scope of this issue, two possible analyses of the link are described in this paragraph, although the Working Group may identify other possible legal analyses. The first is that the digital data is itself a digital asset, and that an analysis that is analogous to that applying to a documentary intangible can apply. Through mercantile usage, and then legislation, a documentary intangible such as a negotiable instrument is a tangible object (a piece of paper) linked to an intangible so that transfer of the instrument transfers the intangible. This type of analysis could apply to a digital asset linked to another asset, although this would entail linking an intangible object (the digital asset) to another intangible (e.g., a debt security) or a tangible object (e.g., gold). The second analysis is to characterise the digital data as constituting an entry on a register which constitutes the root of title to the other asset (so that the data collectively was a title register), or, alternatively, evidence of title. One interesting question is whether, on this second analysis, legislation is necessary to constitute the digital data as the root of title (e.g., as was the case of recent legislation in the U.S. State of Delaware).

89. Finally, addressing the factual and legal relationship between a digital asset and “other assets” must confront an overarching reality: A law governing proprietary interests in digital assets that also would provide that interests in digital assets *ipso facto* determine interests in other assets necessarily would implicate the private law rules governing proprietary interests in every type of other asset that would be affected (not to mention the relevant choice-of-law rules). Such a far-reaching law would seem to be implausible and impractical. But this would be the import of a rule in a law governing digital assets providing that transfer of a digital asset (and the accompanying rights)

¹¹ 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.

¹² In using the word “token” here, this document uses the term in its broadest technical sense to refer to any crypto-asset that exists at least one level in the technology stack higher than the protocol layer, including, but not limited to: ERC-20 standard tokens, ERC-721 non-fungible tokens, and non-native crypto-economic tokens (also called non-native protocol tokens), among others.

carries with it *ipso facto* an interest in the other asset. Of course, transactions outside of the digital asset can be structured so as to reach this result, such as by setting aside the other assets under arrangements that ensure as a matter of contract and other applicable and relevant law that the assets are available for the economic benefit of the holders of the digital assets. This is what is happening (or is assumed or represented to be happening) today. The private law governing digital assets can provide, for example, that an acquirer obtains good title to the digital asset free and clear of conflicting claims. But it cannot as a practical matter ensure that the expected arrangements with respect to the other assets actually have been made and are effective under any potentially applicable law.

90. Regarding the matter of the legal nature of the relationship between the digital data and the other asset (so-called “digital twins”, also referred to as tokenisation of existing assets), the Working Group discussed and agreed upon the need for a thorough consideration of the property rights aspects involved in the link (the term “link” being used here as a functional notion) between digital data and another asset. In particular, the WG considered that there were two possible approaches to this link from a private law perspective: (1) was to consider the link as akin to a negotiable instrument; and (2) was to consider it as akin to a registry; in which case, the question to be considered was how much legislation would be required to support that registry. It was further agreed that much work would be needed on the issue of “digital twins”.

4. Accommodation of disparate types of assets and technologies

91. The challenges in determining the scope of the digital asset project, discussed in II.B. above, are present as well in considering the private law that should be addressed. The Principles to be developed must accommodate quite disparate types of assets and applicable technologies. Moreover, a goal of the Principles will be applicability not only to extant assets and technologies but also to those that will be created and employed in the future.

5. Provision of digital asset custody services

92. At its first session, the Working Group took note of the synergies between intermediated securities work (Geneva Convention) and digital assets work and discussed whether the Project ought to establish minimum standards regarding custodial services (i.e., how the custodian ought to behave and what duties they owed). The WG agreed on the importance of distinguishing between insolvency of the custodian and establishing minimum standards, and it clarified that the private law aspects of custody would be the focus of the WG’s preparations rather than the regulatory questions. It also noted the difference in the position of custodians and clients and that both questions ought to be tackled in the analysis.

93. As part of the intersessional work that the Working Group agreed upon at its first session, Sub-Group 1 was set up to examine questions surrounding control and custody in the area of digital assets (a full list of the participants is available at **Annex 2, Appendix 1**).

94. In terms of substantive discussions, a broad range of issues were covered over the course of SG1’s deliberations. A detailed **work program** was prepared by the co-chairs Louise Gullifer and Luc Thévenoz for the first meeting of the Sub-Group and is available at **Annex 2, Appendix 1**. SG1 in its three meetings considered the questions raised in this work program as well as other issues raised by sub-group members. The approach set out in the first section (limit on our discussion) was, generally, followed. The discussions did not consider digital twins at all, and focused on the ‘cryptocurrency’ paradigm. The Sub-Group had few substantive discussions on the content of ‘control’, although there was some debate of the principle on ‘control’ drafted by Sub-Group 2. Sub-Group 1 has not yet reached a final view on whether the same definition of ‘control’ would work for the purpose of paragraph 1 of Principle Y, as will work for the purposes for which it was developed in Sub-Group 2. This is a matter which the Working Group may wish to consider.

95. The outcome of these meetings was the preparation of the preliminary **Draft Principle Y concerning Custody**, for the consideration of the Working Group, found below.

Principle Y – Custody

1. The holder of a digital asset is the person who, alone or jointly with one or more other persons, has control of that asset under Principle [X] Control.

Explanation

The word 'holder' is used to indicate a person for whom a set of facts is true, that set of facts amounting to sole or joint control of the digital asset. The word is used for at least two reasons. First, it is a word generally used for someone whose relationship to intangibles is the equivalent of possession (such as the holder of a bearer note, the holder of intermediated securities) and seems to already be used in this sense in the digital asset field. Second, it indicates some sort of relationship with the digital asset arising from the factual control.

Multisig wallets do not necessarily mean joint holding. If the holder 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 of that asset.

Question for the Working Group

'Control' in this paragraph is a factual concept. SG2 has a definition of control that refers to the 'exclusive power' to do certain things. We would like to clarify that the word 'power' means the factual power or ability to effectuate the actions listed in (1) to (3).

2. A holder of a digital asset holds as custodian on account of another person (known as the client) if:

(a) the holder 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;

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

(c) the holder 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 this paragraph 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.

This paragraph is definitional of the duties which are owed by a custodian. Thus, if the duties in (a), (b) and (c) are not owed, the holder is not a custodian.

(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 paragraph 4.

This paragraph does not require that a custodian is the sole holder of the digital asset in its custody. Multisig wallets may be used to grant joint control to the custodian and its client. But the client's sole control over the asset would exclude the possibility for the custodian to discharge its duties and therefore would not qualify as a custody relationship.

Figure 3: Principle Y on Custody of Digital Assets

3. 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

This paragraph 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.

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

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

(b) the duty at all times to hold 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 held for the account of clients separate from assets held for its own account;

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

Explanation

This paragraph sets out duties that a state may include. It assumes that a custodian records the assets held 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 paragraph, in addition to the duty to hold assets correlating to those records.

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

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

(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 an omnibus account, where the custodian holds assets for a number of clients. [NOTE: omnibus holdings were present in the MountGox and Cryptopia cases]

(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.

Figure 3: Principle Y on Custody of Digital Assets

5. A digital asset held for a client by a custodian
- (a) may be subject to a security [interest] [right] granted to that custodian by the client;
- (b) may be subject to a security [interest] [right] in favour of that custodian arising by operation of law.

Explanation

This paragraph permits a custodian to have a security interest in the asset it holds 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 discussed in principle []. What the UNIDROIT Securities Convention calls 'security interest' is called a 'security right' in the UNCITRAL Model Law. The Working Group will need to make a choice.

6. A holder is not a custodian of a 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

This paragraph describes the situation where a person (e.g., an exchange) operates in the same way as a bank, in that its clients have a personal claim against it for digital assets that are recorded in accounts associated with those clients. These accounts will record digital assets transferred to the person by the client, or to the person by a third party to be recorded in the account of that client. The person, however, is not a custodian and any digital assets it holds are held on its own account.

7. If a holder enters insolvency proceedings, a digital asset that it holds as a custodian for the account of a client does not form part of the holder'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 holds for clients are not part of the distributed estate. If a holder is not a custodian, any assets it holds will be part of its assets for distribution to its creditors. That will be the case where the holder falls within the situation described in paragraph 6 as well as all situations covered in paragraph 2 other than that of a holder.

Figure 3: Principle Y on Custody of Digital Assets

6. Taking of security over digital assets

96. During its first session, the Working Group discussed whether digital assets were in fact being used as collateral, which was confirmed (more frequently in North America perhaps, but slowly growing in other parts of the world). The WG further agreed that legal structure was not yet established for collateralisation (rules on perfection and priority), and this work could be highly valuable for the financial markets. The WG also examined the concept of "control" in relation to collateralisation of DAs, again drawing parallels with intermediated securities.

97. 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**, and finally, **a series of four draft principles** together with commentary, found below, for the consideration of the Working Group.

I. OUTPUT

98. 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.

II. COORDINATION

A. 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

B. 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>)

III. FOCUS OF SG3’S WORK

99. 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.

IV. MODELS FOR INSPIRATION:

100. 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.

V. USE CASES

101. 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

102. 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).¹³ 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 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

103. 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

104. 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

105. 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.

¹³ A stablecoin can be pegged to a cryptocurrency, fiat money, or to exchange-traded commodities (such as precious metals or industrial metals).

Illustration 5: Central Bank Digital Currencies

106. 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

107. 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).

108. 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.¹⁴ 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.¹⁵ 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.

VI. SECURED TRANSACTIONS PRINCIPLES - STRUCTURE**General notes:**

109. The process to develop one or more scope Principles for secured transactions may be different from the other SGs where they start narrow and build upon that. 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.

110. 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

¹⁴ 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).

¹⁵ See e.g., ISDA *Private International Law Aspects of Smart Derivatives Contracts Utilizing Distributed Ledger Technology: Japanese Law* (Oct 2020) 14-16.

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.

111. 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.

112. 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.

113. 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.

114. 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.

115. 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.

VII. DRAFT PRINCIPLES

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.¹

¹ 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.

Figure 4: Principle A: Secured transaction law applies to digital assets

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.² 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.³

² 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.

³ 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.

Figure 4: Principle A: Secured transaction law applies to digital assets

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”.¹ 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.² 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.³ 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.

¹ 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)).

² 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.

³ 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 created in the grantor’s rights and powers with respect to digital assets

The law should make it simple to create a security right in the digital asset through an agreement between the parties [Note: depending on the structure of these principles, general statements of this nature may or may not be needed in the individual principles.] The law should permit any person to create a security right in a digital asset to secure any type of an obligation, even if the person does not have a right in the digital asset that would qualify as a property right under the generally applicable law, but has a power to transfer control of the digital asset. The law should not require a detailed or technical description of the digital asset in a security agreement, and should automatically extend the security right to any proceeds of the digital asset.

Comments:

While the person would usually be the owner of the asset to be used as collateral, the law should allow a security right to be created in any right in a movable asset.¹ As a consequence, lessees, licensees, and other persons whose interests are short of ownership may create a security right. Such interests may be proprietary or of a contractual nature. Other generally applicable laws may also enable a person to grant a security right in an asset owned by a third party pursuant to an authorization by the owner. The necessity to have an interest or power to transfer an interest in an asset is reflected also in the fact that the grant of a security right over future assets does not create a security right until the person has acquired an interest (or the necessary power) in that asset.

The law should recognize the effectiveness of agreements that provide for the creation of a security right in digital assets described generically, and even by a reference to all assets. Those laws that require specific collateral descriptions may pose challenges to uniquely identifying fungible digital assets. A description of the digital asset that constitutes proceeds of some other collateral should not be required for the security right to continue as long as the proceeds remain identifiable.

Illustration:

A secured creditor takes a hypothec over all intangible assets of a business, including a portfolio of virtual currency. The applicable law requires that each item of the collateral be individually identified in a security agreement. In addition to the secured creditor needing to amend the collateral description each time some virtual currency is sold or acquired, it may not be clear what type of description would sufficiently and individually identify the virtual currency. A description intended to capture all of a party’s bitcoin could provide varying levels of specificity, including “all bitcoin controlled by party X,” “all bitcoin controlled by the following public key addresses,” “the following bitcoin UTXO(s):”

Notes:

Some laws provide that a security right can be created when the person has “rights in the asset to be encumbered” or “the power to encumber it”.² Historically, laws governing specific transactions enabled persons who were not owners of the asset to transfer rights, including by way of security to facilitate commerce. These laws govern transfers made by mercantile agents, factors, or sellers in possession. Where the creation of some type of a security right is conditioned on the person demonstrating its ownership rights, that might complicate the use of digital assets as collateral.

¹ R. Goode, L. Gullifer (n 4) 70.

² UNCITRAL Model Law, art. 6(1).

Figure 6: Principle C: Security rights may be created in the grantor’s rights and powers with respect to digital assets

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.

Figure 7: 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

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

116. 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. (Enforcement of proprietary rights in digital assets outside of insolvency proceedings are discussed below in sub-section D.8.)

117. Given that the private law treatment of digital assets as property may affect whether digital assets belong to a debtor's insolvency estate (see UNCITRAL Legislative Guide on Insolvency Law, Recommendation 35), 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.

118. 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.

119. 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.

8. Remedies and Enforcement

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

121. 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.

122. 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.¹⁶ 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.

123. 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.

9. Law applicable to issues relating to digital assets

124. 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. Only the issues of the applicable law are within the scope of this project, while the other issues are likely to be explored by the Hague Conference on Private International Law or other organisations. 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.¹⁷ 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.

125. 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 the relevant private international law aspects. (A full list of the participants is available at **Annex 2, Appendix 4**).

126. The Working Group is invited to consider and discuss the following preliminary draft principles which were prepared by sub-group 4 co-Chairs Philipp Paech and Elisabeth Noble, and include a number of specific questions for the Working Group to discuss:

¹⁶ See UNCITRAL, Report of the Colloquium on Civil Asset Tracing and Recovery (Vienna, 6 December 2019), para. 25 (UNCITRAL, Feb. 2020).

¹⁷ 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, available at: <https://assets.hcch.net/docs/94e2d886-1cbf-4250-b436-5c1899cb942b.pdf>.

PIL – Tentative Principles (based on the group discussion of and comments on the three scenarios in the previous paper)

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, law governing the system, etc.) can determine the applicable law.

Question for the Working Group: The Working Group is invited to form a view on this, including on whether different fall-back rules are needed for different purposes.

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 party 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 were 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. This subject matter is similar to issues arising and solutions provided in relation to settlement and clearing systems ('Finality'). Finality as an interim solution is granted by a national law, and it is unclear how this will play out in situations involving networks spanning several jurisdictions.

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 or a right to the asset outside the platform?). The private international law question would follow that route. However, that presupposes that a decision is taken regarding which of these two alternatives should be followed). 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.

Question for the Working Group: The Working Group is invited to discuss how the rights to non-native digital assets are to be understood: whether, for instance, as a claim against the intermediary or as a right to the asset outside the platform?

- 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 two unconnected assets economically attributed to different persons. However, the question is: which jurisdiction's law applies. Probably, the more viable solution is to give the law governing the underlying asset priority. This is a typical question for intermediary risk, combined with cross-jurisdictional complications. Solution?

Question for the Working Group: The Working Group is invited to discuss whether the proposed solution of giving the law governing the underlying asset priority over its digital representation (or digital twin) is desirable.

Figure 8: PIL Principles A – B – C

ANNEX I**ADDITIONAL RESOURCES**UNIDROIT Instruments

UNIDROIT, UNIDROIT Convention on International Factoring (1988)

<https://www.unidroit.org/instruments/factoring>

UNIDROIT, UNIDROIT Convention on International Interests in Mobile Equipment (2001)

<https://www.unidroit.org/instruments/security-interests/cape-town-convention>

UNIDROIT, UNIDROIT Convention on Substantive Rules for Intermediated Securities (2013)

<https://www.unidroit.org/instruments/capital-markets/geneva-convention>

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

<https://www.unidroit.org/instruments/capital-markets/netting>

UNIDROIT, UNIDROIT Principles of International Commercial Contracts (2016)

<https://www.unidroit.org/instruments/commercial-contracts/unidroit-Principles-2016>

UNIDROIT, UNIDROIT Legislative Guide on Intermediated Securities (2017)

<https://www.unidroit.org/instruments/capital-markets/legislative-guide>

UNIDROIT, UNIDROIT MAC Protocol (2019)

<https://www.unidroit.org/instruments/security-interests/mac-protocol-2019>

UNCITRAL Instruments

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

<https://uncitral.un.org/en/texts/securityinterests/conventions/receivables>

UNCITRAL Model Law on Secured Transactions (2016)

https://uncitral.un.org/en/texts/securityinterests/modellaw/secured_transactions

UNCITRAL Model Law on Electronic Transferable Records (2017)

https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_transferable_records

Other Organizations

ALI/ELI Principles for a Data Economy, <https://www.ali.org/projects/show/data-economy/>

CoinLaw, mobile app available from the law firm Perkins Coie, <https://appadvice.com/app/perkins-coie-coinlaw/895563535>

European Commission's legislative proposal for markets in cryptoassets,

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593>

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

G7, Investigating the Impact of Global Stablecoins, (G7, IMF, BIS, 2019),
<https://www.bis.org/cpmi/publ/d187.pdf>

G30, Digital Currencies and Stablecoins – Risks, Opportunities, and Challenges Ahead, (G30, 2020),
<https://group30.org/publications/detail/4761>

Global Standards Mapping Initiative (GSMI) Report (2020),
<https://gbbcouncil.org/wp-content/uploads/2020/10/GSMI-Legal-Regulatory-Report.pdf>

HCCH, Convention of 5 July 2006 on the Law Applicable to Certain Rights in Respect of Securities held with an Intermediary (Hague Securities Convention),
<https://www.hcch.net/en/instruments/conventions/full-text/?cid=72>

International Monetary Fund (IMF), Fintech Notes – The Rise of Digital Money, (IMF, 2019),
<https://www.imf.org/en/Publications/fintech-notes/Issues/2019/07/12/The-Rise-of-Digital-Money-47097>

International Monetary Fund (IMF), IMF Policy Paper – Fintech: The Experience So Far, (IMF, 2020),
<https://www.imf.org/en/Publications/Policy-Papers/Issues/2019/06/27/Fintech-The-Experience-So-Far-47056>

International Organization of Securities Commissions (IOSCO), Global Stablecoin Initiatives, (IOSCO, 2020), <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD650.pdf>

International Organization of Securities Commissions (IOSCO), Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms, Final Report, February 2020,
<https://www.iosco.org/library/pubdocs/pdf/IOSCOPD649.pdf>

International Swaps and Derivatives Association (ISDA), reports on collateralised transactions on DLT,
<https://www.isda.org/a/4RJTE/Private-International-Law-Aspects-of-Smart-Derivatives-Contracts-Utilizing-DLT.pdf>

Internet Governance Forum (IGF), Dynamic Coalition on Blockchain Technologies (DC-Blockchain),
<https://www.intgovforum.org/multilingual/content/dynamic-coalition-on-blockchain-technologies-dc-blockchain>

Markets in Financial Instruments Directive (2004/39/EC),
https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-markets/securities-markets/investment-services-and-regulated-markets-markets-financial-instruments-directive-mifid_en

OECD, The Tokenisation of Assets and Potential Implications for Financial Markets, (OECD, 2020),
<https://www.oecd.org/finance/The-Tokenisation-of-Assets-and-Potential-Implications-for-Financial-Markets.pdf>

Stanford Law School's CodeXRegTrax, The Stanford Center for Legal Informatics,
<https://law.stanford.edu/codex-the-stanford-center-for-legal-informatics/regtrax/>

World Bank Group, Distributed Ledger Technology & Secured Transactions: Legal, Regulatory and Technological Perspectives – Guidance Notes Series Note 1: Collateral Registry, Secured Transactions Law and Practice, (WBG, May 2020),
<http://hdl.handle.net/10986/34007>

World Bank Group, 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, (WBG, 2020),
<http://hdl.handle.net/10986/34008>

World Bank Group, Distributed Ledger Technology & Secured Transactions: Legal, Regulatory and Technological Perspectives – Guidance Notes Series Note 3: Distributed Ledger Technology and Secured Transactions Frameworks: A Primer, (WBG, May 2020),
<http://hdl.handle.net/10986/34009>

ANNEX II**INTERSESSIONAL WORK
(JANUARY to MARCH 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)

**SG 1
Work program****1. Limit on our discussion**

In order to get started on our work, we are going to limit it initially to digital assets such as Bitcoin and Ether (what are sometimes called cryptocurrencies), which have no link to other assets (not digital twins). SG2 is going to do the same. The work can then be expanded to consider the application of our conclusions to digital twins.

What amounts to direct holding

A direct holder of a digital asset is a person who has some sort of factual “control” over that asset. However, the concept of control has very diverse meanings in different jurisdictions.

After discussions with SG2, we are going to make an assumption that the best core idea for this type of “control” is the equivalent of possession of the digital asset. Possession is a concept usually applied to tangible assets, but here the idea is that a very similar concept can be applied to the intangible asset we are considering. The exact contours of this concept, and indeed its name, are very much up for debate, but without a starting point we won’t be able to apply this concept to the various possible means of ‘holding’ that exist in the real world. SG1 will seek to develop this concept further in the light of the purpose this concept fulfils in the context of intermediation. SG2 will use the same starting point, but the concept may have a different purpose when considering, for example, transfer to another person or good faith acquisition.

For the purposes of the first meeting, we suggest that we treat “control” as a “black box”, the content of which we will explore once we have debated the other substantive parts of SG1’s remit.

Holder and other people

The holder of a digital asset may hold the asset for its own account or for someone else. A holder for its own account will normally have some sort of proprietary interest in the asset: this could be an absolute interest or a limited interest, such as a security interest. It is possible that a holder for its own account may not have any interest or have a flawed interest because, for example, he is a thief or because the asset was transferred to it by an unauthorised transfer. The legal aspects of these situations are being looked at by SG2.

To approach custody arrangements, SG1 will consider situations where the holder holds for someone else as a result of an agreement.

2. Questions to be addressed

Holding

What facts need to be case for a person to be a 'holder' of a digital asset? (as mentioned above, this question will be addressed later, in the light of our deliberations on the other questions)

Custody

Note on the functional approach: what we call custody (or intermediation, or indirect holding, TDB) here may cover a number of different legal characterisations in national laws (including bailment, trust, etc.). We should aim at defining the main characteristics and legal incidents of custody relationship independently from their legal characterisation.

1. In what situations is a holder a direct holder for its own account and in what situations does it hold for someone else by agreement? Can it be said that the latter situations are all situations of custody? (real life examples to be examined to elucidate this).
2. What is/are the key difference/s between holding a digital asset directly and holding it through a custodian? In particular, how should custody be distinguished from...
 - a. ... provision of (software or hardware) wallet services?
 - b. ... outright transfer of ownership in a similar way as with bank cash deposits?
 - c. ... other situations (which ones)?
3. What are the core duties of a digital assets custodian?
 - a. maintain sufficient holdings in respect of clients' accounts?
 - i. are shortfalls permissible?
 - ii. may the custodian use clients' assets for its own account (see below)?
 - b. allocate assets to clients?
 - c. segregate assets held for clients from assets held for own account?
 - d. general and specific duties of care?
 - e. some fiduciary duties? no-profit? no-conflict?
4. May a client grant the custodian a right of use? **If so**, should the right of use be...
 - a. limited to certain categories of clients?
 - b. subject to duty to provide substitute assets or collateral?
 - c. subject to other requirements (disclosure, compensation, etc.)?
 - d. what are the client' rights in respect of assets used by custodian
 - e. generally, is there a threshold beyond which there is no more custody?
5. Insolvency of custodian
 - a. what should the requirements be for setting (client's) digital assets aside from bankruptcy?
 - b. if there is a shortfall in a particular asset, should it be allocated to clients for whom the custodian is holding this asset or to all custody clients?

List of Participants

Ms Louise GULLIFER <i>Co-Chair</i>	Rouse Ball Professor of English Law University of Cambridge United Kingdom
Mr Luc THEVENOZ <i>Co-Chair</i>	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 <i>Singapore</i>
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 <i>(Observer)</i>	PhD student Université de Genève Switzerland
Mr LIU Hin <i>(Observer)</i>	Oxford DPhil student and a tutor at Oxford and Hong Kong University Fusang
EUROPEAN BANKING INSTITUTE (EBI) <i>(Observer)</i>	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 Work Program

Matthias Haentjens
Charles W. Mooney, Jr.
Subgroup Chairs

The following outline is proposed as a basis for the organization and substance of the work of SG2.

I. Scope of our work—in general.

A. We will address primarily the issues raised in Part D 1, 2, and 3 of the Issues Paper (Study LXXXII – W.G.1 – Doc. 2), with our initial focus on subpart 2 on acquisition, disposition, and competing claims. We should keep in mind that the ultimate goal is to provide guidance to States in adapting their private law to deal with digital assets (DAs). In that connection we are not obliged (nor would it be advisable) to work toward a consensus as to the “correct” resolution of specific doctrinal issues. We should emphasize instead the identification of issues to be addressed and plausible approaches that might be considered.

B. This document is proposed as a starting point for our discussions inasmuch as we must proceed with at least some structure for our work. However, it represents only the initial suggestions of the chairs and its content is entirely open for discussion.

II. Substantive issues to be addressed (not necessarily in the order listed)

A. Which DAs should be covered?

1. Although the scope of the project is not our primary charge, we need some working understandings to ground our discussions.

2. We suggest as a working approach: Base discussions on applicability to some known DAs (e.g., Bitcoin, Ethereum, and possibly other(s) to be discussed), mindful that the ultimate principles must apply broadly and prospectively

3. Down the line the working group will consider how to define the scope of DAs to be covered. For example:

a. Attributes (e.g., Rivalrous? No “double spend”? Public-private key cryptography-based?)

b. Functional (e.g., capable of being subject to “control” as rough analogue or proxy for “possession”?)

B. Methods of transfer (including role of “control”)

1. Transfer outside of relevant DA system (e.g., descent and distribution/inheritance, by will, by other operation of law (statutory liens, judicial liens and decrees), contract between parties, acquisition through custodial/intermediated holding)

a. Our main focus will be on transfers/acquisition within the relevant DA system (including acquisition by a custodian/intermediary)

b. Note: Subgroup 1 will focus on custodial/intermediated holding

Working approach: Base discussions on scenario where Bob acquires Bitcoin by inheritance.

2. Effects of transfer between transferor and transferee (e.g., *nemo dat* and shelter principle) and as against third parties (e.g., negotiability, finality, takes-free/innocent acquisition rule)

Working approach: Base discussions on scenario where Bob transfers Bitcoin to Alice, and Carol asserts a competing claim.

3. Standards for finality and takes-free/innocent acquisition rules (e.g., no wrongful knowledge/notice, good faith, “control” as proxy for delivery/possession, *sui generis* standards vs. incorporation of existing standards vs. combination)

Working approach: Same as for B.2.

4. Coordinate with priority principles for secured transactions addressed by Subgroup 3

Working approach: Base discussions on scenario where Bob transfers Bitcoin to Alice, and Carol asserts a pledge on the Bitcoin.

5. Broad conception of “transfer” (See Issues Paper at 9 and note 4)

C. Definition/characteristics of “control”

1. Compare to standards for delivery or possession

2. *Purpose* of control should dictate its attributes

3. Working hypothesis: control is a condition for qualifying for innocent acquisition protection (and possibly super-priority for security rights)

4. Working Approach: Base discussions on the following attributes:

a. Power to receive benefits and power to block others from receiving benefits

b. Power to transfer control (or practical equivalent for new DA that derives from previous DA)

c. Control person’s power to identify itself as being in control

d. Must powers be exclusive? If so, does sharing power (e.g., multi-sig arrangements) destroy control?

D. “Tethering” or “digital twins”

1. Should a *law on DAs* (our principal focus) provide that transfer of a DA *ipso facto* may transfer rights in tethered asset?

2. If so, under what circumstances/conditions?

3. If so, how are rights of third parties under other applicable law addressed?

4. Should takes-free rule for DAs extend to tethered assets?

5. If so, under what circumstances/conditions?

3. Should *ipso facto* treatment be left to other law outside of law on DAs?

III. Initial work product to be developed by Subgroup 2

1. Coordinate with Secretariat and other subgroups

2. Provide examples of potential principles to be included in the ultimate guidance document?

List of Participants

Mr Matthias HAENTJENS (<i>Co-Chair</i>)	Professor of Law Leiden University the Netherlands
Mr Charles MOONEY Jr. (<i>Co-Chair</i>)	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 Kozolchuk 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 (<i>Observer</i>)	Attorney at Law Carlton Fields United States of America
AMERICAN LAW INSTITUTE (ALI) (<i>Observer</i>)	Mr Steven WEISE Partner United States of America
LAW COMMISSION OF ENGLAND AND WALES (<i>Observer</i>)	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) (<i>Observer</i>)	Mr Matthias LEHMANN Professor Universität Wien EBI German

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)

List of Participants

Mr Marek DUBOVEC (<i>Chair</i>)	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) (<i>Observer</i>)	Mr Klaus LÖBER Head of Oversight DG Market Infrastructure and Payments Germany
HAGUE CONFERENCE ON PRIVATE INTERNATIONAL LAW (HCCH) (<i>Observer</i>)	Ms Gérardine GOH ESCOLAR First Secretary Permanent Bureau the Netherlands
KOZOLCHYK NATIONAL LAW CENTER (NatLaw) (<i>Observer</i>)	Mr Bob TROJAN Senior Advisor United States of America
UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAW (UNCITRAL) (<i>Observer</i>)	Mr Jae Sung LEE Legal Officer International Trade Law Division Austria
AMERICAN LAW INSTITUTE (ALI) (<i>Observer</i>)	Mr Steven WEISE Partner United States of America
Mr Andrew (Drew) HINKES (<i>Observer</i>)	Attorney at Law Carlton Fields United States of America
EUROPEAN BANKING INSTITUTE (EBI) (<i>Observer</i>)	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 (<i>Co-Chair</i>)	Associate Professor London School of Economics & Political Science Germany
EUROPEAN BANKING AUTHORITY (EBA) (<i>Observer</i>) (<i>Co-Chair</i>)	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) (<i>Observer</i>)	Ms Gérardine GOH ESCOLAR First Secretary Permanent Bureau the Netherlands
KOZOLCHYK NATIONAL LAW CENTER (NatLaw) (<i>Observer</i>)	Mr Bob TROJAN Senior Advisor United States of America
UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAW (UNCITRAL) (<i>Observer</i>)	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