



EN

**Digital Assets and Private Law
Working Group**

UNIDROIT 2022
Study LXXXII – W.G.6 – Doc. 3

Sixth session (hybrid)
Rome, 31 August – 2 September 2022

English only
August 2022

ISSUES PAPER

1. This Issues Paper is a track changes version of the UNIDROIT Digital Assets and Private Law (DAPL) Principles. The changes tracked are those made in between the Working Group's 5th Session (7-9 March 2022) and 6th Session (31 August – 2 September 2022). The starting point for this document was a clean (with all changes accepted) version of [Study LXXXII – W.G.5 – Doc. 2](#) which has been contrasted with the draft of the Principles produced at the conclusion of the 9th Session of the DAPL Drafting Committee (12 August 2022). This clean draft can also be found as Document 2 of this meeting.

2. This document goes Principle by Principle and includes a set of notes/explanations at the end of each Principle detailing the reasoning behind the changes which have been proposed in intersessional discussions. These changes were the result of one of the following activities:

- a. The deliberations which took place at the Working Group's 5th Session (WG5). All of these were captured in [Study LXXXII – W.G.5 – Doc. 4: Draft Summary Report of the 5th session.](#)
- b. The discussions of the Drafting Committee which met 5 times since the last meeting of the Working Group:
 - i. Drafting Committee Session 5 (DC5) took place on 25 March 2022. The session was dedicated to a discussion of the outcomes of WG5 and the allocation of future work before the 101st Session of the UNIDROIT Governing Council and upcoming Drafting Committee sessions. The consistency of the Principles was discussed together with a redrafted version of the Principle on Conflict of Laws, its structure and, particularly, the bottom of the waterfall, and newly drafted Principle (bis) and Principle (quarter) for this section.
 - ii. Drafting Committee Session 6 (DC6) took place on 8 April 2022. The session was focused on the refinement of the Principles on: on Scope, Definitions, General Principles, Definition of Control, Identification of a Person in Control of a Digital Asset, and the Innocent Acquisition Rule. Future work was allocated among the Members of the Drafting Committee in relation to several other Principles and a revision of the accompanying Commentary was also requested.
 - iii. Drafting Committee 7 (DC7) took place on 25 April 2022 and focused on discussions of a newly revised draft of Principle 5, amendments to the Principle on Definitions, General Principles, Principle 7 and Principle 8 and updates to the Commentary.

- iv. Drafting Committee 8 (DC8) took place on 24 June 2022. The session paid special attention to the Governing Council Meeting held on 8-10 June 2022, particularly, the concerns raised by several Governing Council Members relating to the functional notion of control. The Drafting Committee Members were informed of the feedback from the Steering Committee and agreed on inter-sessional work to incorporate the comments.
- v. Drafting Committee #9 (DC9) took place on 12 August 2022. The session focussed on preparing a draft for WG6, including making final adjustments to the Principles on Secured Transactions, Custody, Enforcement, and some others. Consideration was also given to parts of the Commentary which had been updated by various members of the Drafting Committee.
- c. The input received from the DAPL Steering Committee: Following a mandate from the Working Group, a draft of the Principles was shared with the Steering Committee in March-April 2022 alongside questions for which feedback was requested. 24 experts from 14 countries and one Regional Economic Integration Organisation provided comments. All of these can be found in Annex 1 of this document.
- d. The comments received as part of the discussions at the 101st Session of the UNIDROIT Governing Council, where the Principles were presented.
- e. A Special Workshop on Issues Related to Enforcement in Digital Assets , which took place as a side event to the 101st Session of the UNIDROIT Governing Council in Rome and on Zoom on 10 June 2022. The Workshop was attended by Members of the UNIDROIT Governing Council, the UNIDROIT Working Group on Digital Assets and Private Law, the UNIDROIT Working Group on Best Practices in the Field of Effective Enforcement, as well as Members of the Steering Committee of the Working Group on Digital Assets. A summary Report of this Workshop is found here <https://www.unidroit.org/workshop-on-issues-related-to-enforcement-in-digital-assets/>
- f. Some general efforts of the Drafting Committee and the Secretariat to prepare a more consistent and cleaner set of Draft Principles, with a view towards moving towards the finalisation of the document.

MASTER COPY OF THE DRAFT PRINCIPLES AND COMMENTS

Table of contents

INTRODUCTION

SECTION I: SCOPE AND DEFINITIONS

- Principle 1: Scope ~~[of the principles]~~
- Principle 2: Definitions
- Principle 3: General principles
- Principle 4: ~~Digital Assets 'linked' to Other Assets~~ [Linked assets](#)

SECTION II: PRIVATE INTERNATIONAL LAW

- Principle 5: Conflict of ~~L~~ [laws](#)

SECTION III: CONTROL

- Principle 6: Definition of ~~C~~ [control](#)
- Principle 7: Identification of a ~~P~~ [person](#) in ~~C~~ [control](#) of a ~~Digital Asset~~ [digital asset](#)

SECTION IV: TRANSFER

- Principle 8: Acquisition and ~~D~~ [disposition](#) of ~~Digital Assets~~ [digital assets](#)
- Principle 9: Innocent ~~Acquirer Rule~~ [acquisition rule](#)
- Principle 10: Shelter ~~principle~~ [rule](#)
- Principle 11: Application of ~~Innocent Acquirer Rules to a Custody Relationship~~ [innocent acquisition rule to a custody relationship](#)

SECTION V: CUSTODY

- Principle 12: Custody
- Principle 13: Duties owed by a ~~C~~ [custodian](#) to its ~~C~~ [client](#)
- Principle 14: Other ~~A~~ [aspects](#) of ~~C~~ [custodianship](#)
- Principle 15: ~~Sub-Custody~~ [Insolvency of a custodian](#)

SECTION VI: ~~COLLATERAL~~ [SECURED](#) TRANSACTIONS

- Principle 16: ~~Collateral Transactions~~ [Secured transactions](#): General
- Principle 17: Control as a ~~Method of Achieving Third-Party Effectiveness~~ [method of achieving third party effectiveness](#)
- Principle 18: Priority of ~~Security Rights~~ [security rights](#) in ~~Digital Assets~~ [digital assets](#)
- Principle 19: Effective ~~E~~ [enforcement](#) of ~~Security Rights~~ [security rights](#) in ~~Digital Assets~~ [digital assets](#)

SECTION VII: ENFORCEMENT

- [Principle 20: Enforcement](#)
-

SECTION VIII: INSOLVENCY

- Principle ~~{20}1~~ [1](#): Effect of ~~I~~ [insolvency](#) on ~~P~~ [proprietary](#) [and ~~Security] Rights~~ [security](#)] [rights](#) in ~~Digital Assets~~ [digital assets](#)

Issues Paper Continued:

3. The structure of the Principles has remained largely unchanged between WG5 and WG6. Consideration was given to incorporating Principle 4 on Linked Assets into Principle 3(3). However, it was recommended at DC9 to retain it as a separate Principle in order to highlight this important point separately and with dedicated detailed Commentary.

4. Additionally, the Principle on Sub-Custody has been incorporated into different parts of Section V which deals with Custody. Instead, Principle 15 now relates to 'Insolvency of custodian'.

5. As a general point, it is noted that the terms 'the law should provide that' have been removed from the Principles based on discussion on this matter at WG5 and several DC meetings.

INTRODUCTION

I. Reasons for the Principles

1. These Principles are designed to facilitate transactions in digital assets of the type covered by the Principles, which are briefly described below. These are types of digital assets often used in commerce.

2. For transactions in these types of digital assets to have the maximum efficiency, it is important to have clear rules that apply to the key aspects of these transactions (briefly described below). Without predictable results, the transactions will have inherent inefficiencies and there will be a reduction in the value of the transactions in commerce.

3. It is intended that these Principles will provide guidance to principals in the transactions covered by these Principles, their advisors (including lawyers), and the courts and others who will consider the legal effects of these transactions. [In sum, these Principles aim to reduce legal uncertainty which practitioners, judges, legislators, and market participants would otherwise face in the coming years in dealing with digital assets.](#)

~~3.4.~~ It is recommended to States to adopt legislation consistent with these Principles. This will have several benefits: it will increase the predictability of transactions involving these assets that occur in that State. In addition, as these transactions frequently involve persons in different States, the greater the consistency among States, the greater the predictability in cross-border transactions. [See also Principle 3.](#)

II. [Neutrality and the Relationship of Principles to National Law](#)

5. These Principles take a practical and functional approach. This has several important ramifications. First, these Principles are technology and business model neutral. In several instances the commentary to these Principles refers to, and uses examples that draw on blockchain technology or distributed ledger technology. However, this has been to only clarify the application of the Principles, and is not meant to modify or undermine the applicability of these Principles to digital assets that employ other technologies. Importantly, this is not meant to impair the technology neutrality of these Principles. Thus, these Principles are intended to apply to all Digital Assets (as defined in these Principles), whether or not the record of these Digital Assets is on a blockchain. On the scope of these Principles, and more specifically, the type(s) of digital assets these Principles cover, see immediately below, under III. Scope of Principles. On the definition of Digital Assets, see Principle 2(2).

6. Second, these Principles are jurisdiction neutral. Therefore, these Principles have not been drafted with the terminology of a specific jurisdiction, and are intended to be applied to any legal system or culture. This means that they are intended to facilitate the legal treatment of digital assets in both common law and civil law systems. The concept of control used in these Principles, for instance, is not intended to be understood as 'control' as used in certain common law jurisdictions. Also, while being akin to the concept of 'possession' as used in certain civil law jurisdictions, control as used in these Principles must not be understood to be identical to such possession: where in civil law jurisdictions a possessor may 'hold' an asset through another person, under these Principles a person cannot control a Digital Asset through another person unless the criteria of Principle 6 are met. See below, Principle 6.

7. The jurisdiction neutrality of these Principles as explained above also means that it is for the jurisdiction in question to decide, how to implement these Principles into its own law(s). Traditionally, common and civil law jurisdictions use different strategies to regulate new phenomena and to

implement supra-national law, and these Principles do not prescribe a specific strategy. A common law jurisdiction, for instance, may elect – in line with its tradition to do so – to adopt a specific statute that is consistent with, or implements these Principles as a whole. Alternatively, a civil law jurisdiction may elect to implement these Principles into existing laws and amend those as appropriate. These Principles thus take no position as to whether its rules should be included in a State’s special law on digital assets, incorporated into more general laws, already follow from general laws, or are addressed by a combination of these approaches.

8. Third, these Principles are organisationally neutral. This means, as already stated above, that these Principles take no position as to in what part of a State’s laws its rules should be included. Thus, a State may implement these Principles into a specific law on digital assets, but a State may also consider these Principles to follow from rules of general private law, commercial law or consumer law. However, the organisational neutrality of these Principles does not mean that they can be implemented so that their scope be more limited than defined in these Principles. For instance, if a certain jurisdiction considers ‘commercial law’ to apply to merchants only and not to consumers, these Principles cannot be implemented into that jurisdiction’s commercial law only, because the scope of these Principles does not exclude consumers. Vice versa, these Principles cannot be implemented into a jurisdiction’s consumer law only, because the scope of these Principles is not limited to consumers.

9. The organisational neutrality of these Principles also does not mean that they are intended to be implemented outside of private law. These Principles cover only private law issues relating to digital assets and, in particular, proprietary rights. Thus, they specifically address digital assets where these are the object of dispositions and acquisitions, and where interests in those assets are to be asserted against third parties. As a matter of principle, they do not cover rules that are to be enforced by public authorities which in many jurisdictions would be called ‘regulation’ or ‘regulatory law’. For instance, these Principles do not cover such matters as when or whether a person must obtain a licence for engaging in activities that concern digital assets. In the same vein, they do not cover rules for how persons should hold digital assets, if compliance with those rules is sanctioned by public authorities.

~~4.10. Moreover, These Principles apply~~ these Principles intend to only regulate a specific area of private law, and there are many issues of private law which are not addressed by the Principles. These issues concern, for instance, rules of private law relating to intellectual property or consumer protection. As a matter of principle, these areas of law are not addressed by these Principles, and national intellectual property and consumer protection laws therefore remain unimpaired by them. Also, these Principles do not address many issues of private law relating to contract and property law. Examples of these issues not addressed by these Principles include whether a proprietary right in a digital asset has been validly transferred to another person, whether a security right in a digital asset has been validly created, the rights as between a transferor and transferee of a digital asset, the rights as between a grantor of a security right in a digital asset and the relevant secured creditor, in general the legal consequences of third party effectiveness of a transfer of digital assets, the requirements for, and legal consequences of, third party effectiveness of a security right in a digital asset, etc. etc. See also Principle 3(3) and Principle 4. In sum, these Principles use certain core concepts (described below) and do not attempt to address all contractual and proprietary issues relating to the digital assets covered by the Principles. As States may have a wide range of other laws (in statutes and court decisions), there is no attempt to identify the specific law that may apply.

~~If a State were to adopt a statute or statutes consistent with these Principles, it should determine whether it would be most effective to adopt a complete standalone law which covered all of the matters addressed in these Principles or whether to amend existing laws as appropriate.~~

III. Scope of Principles

~~5.~~11. These Principles apply only to a subset of digital assets. These are digital assets that are frequently used in commerce. They are distinguished from other digital assets by identifying them as digital assets that are subject to control (as briefly discussed below). [Principle 2\(2\)](#). For these Principles, 'control' refers to a digital asset where a person can establish that it has (i) the exclusive ability to change the control of the digital asset to another person, (ii) the exclusive ability to prevent others from obtaining substantially all of the benefit from the digital asset; and (iii) the ability to obtain substantially all the benefit from the digital asset (**see Principle 6: Definition of Control**).

~~6.~~12. These Principles apply only to core transactions in the covered digital assets – outright transfers and transfers for security.

~~7.~~13. In some cases a digital asset covered by the Principles will state that it is 'linked' to another asset.⁴ As discussed above in connection with the relationship to national law, law other than these Principles will determine the contractual and proprietary effects (if any) of the link to another asset (**see Principle 4: Digital Assets 'linked' to other assets**).

IV. Core concepts

14. Proprietary aspects. These Principles treat digital assets as having proprietary characteristics, without addressing whether they are considered 'property' under the other law of a State. [See Principle 1: Scope and Principle 3\(1\): General Principles](#).

~~8.~~15. Private international law. Given the intangible nature of the digital assets and that many transactions occur without a physical location and taking into account the need for certainty in determining the applicable law, the Principles give significant effect to party autonomy. ~~([See Principle 5: Private International Law](#))~~.

~~9.~~16. Control. As discussed above in connection with the description of which digital assets are ~~addressed~~[covered](#) by ~~this law~~[these Principles](#), the concept of 'control' plays a critical role in these rules (see discussion of transfer below). [See Principles 6 -7 \(Section III: Control\)](#).

17. Transfer [and secured transactions](#). As noted above, these Principles cover only that set of transactions most important in commerce – outright transfers and transfers for security. As part of the Principles, an innocent transferee who has control and meets certain additional requirements, will take the digital asset free of property claims to it. In addition, a secured creditor that has control of a digital asset will have priority over other secured creditors with a security right in the same digital asset. These rights will benefit subsequent transferees under a 'shelter' rule ~~([see](#) [See Principles 8 -11 \(Section IV: Transfer\)](#))~~ and [Principle 16 - 19 \(Section VI: Secured Transactions\)](#).

~~10.~~18. Custodians. The digital assets addressed by these Principles will often be held by custodians. The Principles address the role of custodians with respect to the transfers addressed by these Principles. [See Principles 12-15 \(Section V: Custody\)](#).

V. Transition rules

~~11.~~19. Generally, these Principles would apply only prospectively. This would protect existing transactions and legal relationships. There are some instances where, after a 'grace period' some of the Principles could apply to existing transactions.

Continued Issues Paper

6. The introduction to the Principles is designed to guide any reader towards developing an understanding of what the Principles relate to, and how they are broadly structured. Some non-substantive changes were made to the Introduction to include more cross references.

7. All the substantive changes to the Introduction were proposed at DC9. These changes are mainly the result of queries from the Members of the Steering Committee which sought additional clarification as to the items covered in Principles 1-3.

8. In this regard, an additional sentence has been added to Part I of the introduction to clearly set out the purpose of the Principles. This sentence was originally part of the Commentary for Principle 1.

9. Additionally, Part II has been redrafted with a greater focus on technological, jurisdictional, and business model neutrality. These changes also make the Introduction completely consistent with the rest of the Principles.

10. As part of this redrafting, additional explanations have been included with regard to the concept of 'control' as referred to in the Principles, which is not intended to be understood as 'control' as used in certain common law jurisdictions. Additionally, it should not also be understood to be identical to 'Possession' in certain civil law jurisdictions. Furthermore, guidance is provided on how jurisdictions might consider implementing these Principles domestically.

11. Additionally, the Introduction also highlights neutrality in terms of the organisational approach which States might adopt to implement them. Several paragraphs in the Introduction now explain what this means, and what this does not mean.

12. Finally, the redraft of the Introduction adds further emphasis on the fact that these Principles only apply to the private law elements of digital assets.

SECTION I: SCOPE AND DEFINITIONS

Principle 1: Scope ~~{of the principles}~~

These Principles deal with the private law relating to ~~{transactions in}~~ digital assets.

Commentary

1. These Principles are meant to serve as guidelines for States to enable their private laws to be consistent with best practice and international standards in relation to the holding, transfer and use of digital assets, as defined in Principle 2(2~~3~~). They cover only private law issues relating to digital assets and, in particular, proprietary rights.¹ Thus, they specifically address digital assets where these are the object of dispositions and acquisitions, and where interests in those assets are to be asserted against third parties. As a matter of principle, they do not cover rules that are to be enforced by public authorities (which in many jurisdictions would be called 'regulation') ~~– or 'regulatory law'~~. For instance, these Principles do not cover such matters as when or whether a person must obtain a licence for engaging in activities that concern digital assets. In the same vein, they do not cover rules for how persons should hold digital assets, if compliance with those rules is sanctioned by public authorities ~~–~~.

~~2.~~ Moreover, these Principles intend to only regulate a specific area of private law, and there are many issues of private law which are not addressed by the Principles. These issues concern, for instance, rules of private law relating to intellectual property or consumer protection. As a matter of principle, these areas of law are not addressed by these Principles, and national intellectual property and consumer protection laws therefore remain unimpaired by them. Also, these Principles do not address many issues of private law relating to contract and property law. Examples of these issues not regulated by these Principles include whether a proprietary right in a digital asset has been validly transferred to another person, whether a security right in a digital asset has been validly created, the rights as between a transferor and transferee of a digital asset, the rights as between a grantor of a security right in a digital asset and the relevant secured creditor, the legal consequences of third party effectiveness of a transfer of digital assets, the requirements for, and legal consequences of, third party effectiveness of a security right in a digital asset, etc. etc. See also Principle 3(3) and Principle 4.

~~2-3.~~ These Principles address situations where gaps may exist in current (private) laws, and also where traditional approaches would not be appropriate and should be modified. However, these Principles take a practical and functional approach in that they are intended to facilitate the private law treatment of digital assets in ~~both common-law~~ technological and ~~civil-law~~ legal systems. ~~They are not jurisdiction specific, and can be applied to any legal system or culture. They address situations where gaps may exist in current law, and also where traditional approaches would not be appropriate and should be modified.~~² However, as is made clear in the Principles and commentary, there are many issues of private law which are not addressed by the Principles. ~~The~~ Thus, the internationality of the Principles will 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.³ On the technological, jurisdiction and organisational neutrality of these Principles, see more extensively above, under Introduction, Part II. Neutrality and the Relationship of Principles to National Law.

¹ Cf. UNIDROIT 2021 – Study LXXXII – W.G.4 – Doc. 2, Issues Paper, p. 8.

~~² UNIDROIT 2021 – Study LXXXII – W.G.4 – Doc. 2, Issues Paper, p. 8.~~

³ UNIDROIT 2021 – Study LXXXII – W.G.4 – Doc. 2, Issues Paper, p. 4.

~~3. In sum, these Principles aim to reduce legal uncertainty which practitioners, judges, legislators, and market participants would face in the coming years in dealing with digital assets.⁴~~

~~[maybe examples of digital assets here, or in Introduction]~~

~~⁴ UNIDROIT 2021 – Study LXXXII – W.G.4 – Doc. 2, Issues Paper, p. 5.~~

Continued Issued Paper

13. The deletions of the two bracketed texts in this Principle have been the result of deliberations on this point at WG5 and DC6. At WG5 it was noted that the use of the words 'deal with the private law' was sufficient to indicate to readers what the scope of the Principles related to.

14. At DC6, consideration was also given to other words in this Principle, including 'related to', replacing 'to' with 'of', and removing 'the'. However, in order to offer the greatest amount of clarity, specificity, and being comprehensive and inclusive, the present version of the Principle was approved.

15. The additions to the Commentary are for the purposes of providing more elaboration and clarity. This elaboration relates to the applicability of the Principles to private law, and what that means. This can be found in Paragraph 2 of the Commentary.

Principle 2: Definitions

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

1. 'Electronic records' comprise a class of which 'digital assets' (as defined in ~~p~~ Principle 2(2)) form a subset. As defined, an 'electronic record' consists of information stored in an electronic or ~~other intangible medium, which is capable of being retrieved.~~ digital medium, which is capable of being retrieved. 'Electronic medium' must be understood in a broad sense. Thus, the definition is intended to include any type of digital technology, even if the storage itself may not rely on electrons, such as hard disks use magnetic fields, DVDs use physical changes in the material. It is implicit in the requirement that the information be retrievable that the information also must be retrievable in a form that can be perceived. It follows that an electronic record would not include, for example, oral communications that are not stored or preserved or information that is retained only through human memory.

2. This definition is consistent with the definition of the term 'electronic record' in Article 2 of the UNCITRAL Model Law on Transferable Records and similar definitions in various national laws.⁵ ~~{~~Were it not for this provenance of the definition it might seem ~~quite~~ odd that the term 'electronic record' is defined as 'information' and not as a 'record' of information (except as might be implicit in the requirement that the information be stored and retrievable). If one were writing on a clean slate, perhaps it would make sense to use the "record of information" formulation. However, the role of this term is solely as a component of the definition of 'digital asset'. As explained in the commentary to the definition of 'digital asset', the determinative factor is whether an 'electronic record' is capable of being subject to control'. It follows that either formulation of the definition of 'electronic record' would produce the same result. ~~Given that, it is appropriate and prudent to adopt the approach to~~ Therefore, the definition of the term has been chosen that already has been generally accepted~~}.}~~

(2) ~~{Controllable}~~ 'Digital asset' means an electronic record which is capable of being subject to control.

3. The definition of 'digital asset' includes an electronic record only if it is 'capable of being subject to control'—as 'control' is defined in Principle 6. For example, some electronic records might be described colloquially as 'digital assets', but normally could not be subjected to 'control', as defined, and consequently would not be digital assets as defined here. While reference is made to Principle 6 for a detailed explanation of the concept of control used here, it should be stated already here that 'control' as defined in these Principles means exclusive, i.e. non-rivalrous control.

4. Consider a simplified example: Two sets of information compose an electronic record. One set is ~~'No Left Turn Unstoned' (NLTU)~~ Information Set Alpha' (IS Alpha) plus ~~information (key information)~~ that, pursuant to public-key cryptography, renders this set of information capable of being subject to control by means of the associated private key. (Note that this does not mean that the key information necessarily contains the private key itself, but only the information that makes it controllable with the private key.) Those two components—~~NLTU~~ IS Alpha plus the key information—compose the digital asset (the ~~'NLTU~~ IS Alpha digital asset'). The second set of information is ~~'I Gave Her the Ring, She Gave Me the Finger' (IGHTR, SGMTF)~~ Information Set Beta' (IS Beta). Although information consisting of ~~IGHTR, SGMTF~~ IS Beta is associated with and included in the same electronic record as the ~~NLTU~~ IS Alpha digital asset, a transfer of control of the ~~NLTU~~ IS Alpha digital asset so that it becomes subject to control through different key information would not transfer control of the ~~IGHTR, SGMTF~~ IS Beta information. Indeed, the ~~IGHTR, SGMTF~~ IS Beta information is not (it is assumed) capable of being subject to control. This example is not unrealistic.

⁵ See, e.g., Uniform Electronic Transactions Act (United States), Article 2(7) (defining 'electronic record'), 2(13) (defining 'record')

For example, an interest in Bitcoin is composed of an unspent transaction output (UTXO). The UTXO might be associated with information, such as information included in a header, that is a part of the same electronic record as the UTXO but which is not capable of being subject to control. The header information would not necessarily be transferred as a result of spending the UTXO.⁶

5. Continuing with the example of the NLTU-IS Alpha digital asset described in comment 24, pursuant to Principle 9 an innocent acquirer (IA) of the NLTU-IS Alpha digital asset would acquire it free of conflicting proprietary claims. But this would not mean that the IA acquires the information NLTU-IS Alpha (e.g., that the IA 'owns' NLTU-IS Alpha, even assuming that such information could be 'owned' under the applicable law). Instead, the IA acquires the information NLTU-IS Alpha only insofar as it is associated with the key information as a part of the NLTU-IS Alpha digital asset. The information NLTU-itself-IS Alpha presumably exists not only as a component of the NLTU-IS Alpha digital asset but also independently and separate and apart from the NLTU-IS Alpha digital asset. The information NLTU-IS Alpha is the same—'No-Left-Turn-Unstoned-IS Alpha' is 'No-Left-Turn-Unstoned-IS Alpha'—however or wherever that information might be stored, existing, or perceived. The NLTU-IS Alpha digital asset is distinct, however, because it is composed not only of the information NLTU-IS Alpha but also of the key information.

6. The information NLTU-IS Alpha might be an image, poem, book, video, song, database, a combination of 1s and 0s without any inherent value, or any other type of information. But whatever its content or characteristics, under these Principles law (see Principle 2(3), defining 'Principles law') the information would remain subject to any applicable laws other than ~~law governing digital assets contemplated by these~~ the Principles (digital assets law). If the information were subject to valid copyright protection, for example, the rights of the holder of the copyright would not necessarily be affected by the creation, acquisition, or transfer of the digital asset.⁷ See Illustration {2}, *infra*. On the other hand, it is possible that inclusion of information in a digital asset, or the use, transfer, or acquisition of the digital asset, could violate or infringe upon rights under such laws. Even if the information NLTU-IS Alpha (or any other information included in a digital asset) were not subject to any protection under intellectual property or other laws, the existence, use, or rights (if any) in respect of that information outside of and other than as a part of a digital asset would not be affected by ~~a digital assets~~ the Principles law.

7. The Illustrations to Principle 1 (~~scope of the Principles~~), Principle 2(1) (definition of 'electronic record'), and Principle 2(2) (definition of 'digital asset'), *infra*, provide additional examples of the application of the definition of digital asset and the scope of these Principles.

Illustrations of the application of Principle 1 (~~scope of the Principles~~), Principle 2(1) (definition of 'electronic record'), and Principle 2(2) (definition of 'digital asset')

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

8. In a public blockchain no one person controls the underlying protocol (software)—ie, the blockchain that tracks transactions in the digital assets. A consensus mechanism embedded in the protocol verifies the validity of transactions that users attempt to effect through the protocol. No one individual user has control over the protocol or its consensus mechanism. The underlying protocol (system) for the public blockchain would not be capable of being subject to "control" as defined in

⁶ Examples and discussion in these Principles that draw on blockchain technology or distributed ledger technology generally are not intended to modify or undermine the applicability of these Principles to digital assets that employ other technologies or to impair the technology neutrality of these Principles. This is a general point that is not limited to the discussion here of the definition of 'digital asset'.

⁷ ~~The following sentence was in the original commentary but the paragraph from the Transfer Principle has now been taken out. [Consistent with this analysis, under [Transfer] Principle [X.2](11) a digital assets law adopting these Principles should be made subject to any conflicting provisions of any applicable intellectual property laws (among other laws that a State might specify).]~~

Principle ~~X.1.D.6~~). However, an individual user does have control over a private keys, which allow the individual user to obtain 'control' (as so defined) over a digital asset within the protocol (ie, over a UTXO (unspent transaction output) in the case of ~~B~~bitcoin).

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

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

Illustration 2: Digital if a digital asset contains information that is a valuable dataset/database (eg, e.g., dataset that is the basis for the operation of an AI system), image, or textual expression, the information is subject to applicable intellectual property laws and the information existing outside of the digital asset is not part of the digital asset.

11. ~~If~~As discussed above in paragraph 6, if the information included in the digital asset is itself subject to protection under intellectual property law (presumably copyright law, in this example), the rights of the holder of the intellectual property would be preserved notwithstanding the inclusion of the information in the electronic record or the transfer of the digital asset to an innocent acquirer. To the extent permitted by the applicable intellectual property law the transferee of the digital asset might be entitled to the use and enjoyment of the information (not unlike the lawful purchaser of a book protected by copyright). Alternatively, if the information or its functionality were protected by patent law, for example, then the acquirer of the digital asset could be infringing the patentee's rights by using the information.

12. Although the particular facts of this illustration may not be realistic or reflect common practice, it is intended to illustrate and underscore the point that ~~a~~the Principles law and other law relating to digital asset law assets should be subject to any applicable intellectual property laws. It also illustrates the broader point that a digital asset comprises only the package of information that includes the information necessary to make it capable of being subject to control. ~~The~~As discussed above in paragraph 5, the same information that is included in a digital asset and that exists ~~outside of and separate and apart from the digital~~Illustration 2: Digital asset contains information that is not a part of valuable dataset/database (eg, dataset that is the digital asset basis for the operation of an AI system), image, or textual expression.

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

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

~~The digital asset is composed only of information capable of being subject to control and the other asset (even if it is itself composed of information) is not a component of the digital asset and is not within the scope of these Principles. For example, under a law conforming to Principle 9, an innocent acquirer of the digital asset may take the digital asset free of competing proprietary claims. But other law (and the relevant facts, including the applicable contractual arrangements) would determine whether (and the extent to which) or not the acquirer would take free of (or subject to) competing proprietary claims to the other asset.~~

Illustration 4: A Facebook page with password for access is not a digital asset.

13. Generalizations about social media/social networking platforms are difficult. But Facebook and many other social media platforms generally involve licensing arrangements with users that do not permit the users to acquire ‘ownership’ of ‘pages’ or the data stored on the platform. This is so even though colloquially users may refer to ‘their’ pages and information that ‘belongs’ to them. In general, these platforms do not allow users to acquire the exclusive abilities contemplated by the definition of ‘control’ in Principle 6 ~~definition of ‘control’~~. Consequently they do not constitute or involve digital assets within the scope of these Principles.

Illustration 5: Although an Excel or Word file with password protection could be a digital asset, the Principles law would have no material impact or utility for such assets.

14. A Word, Excel or similar data file recorded in a hard drive is an electronic record as defined in Principle 2(1). If access to viewing the contents of the file is password protected, then it is possible that one who has both knowledge of the password and direct access to the hard drive in which the file is stored would have the exclusive abilities necessary to obtain control under Principle 6. Because the file would be capable of being subject to control, the file would be a digital asset as defined in Principle 2(2) and within the scope of these Principles. That said, unless the digital asset were associated with a protocol that facilitates the acquisition and disposition of such assets, ~~laws adopting these Principles would not have any material utility or impact for these assets.~~ the Principles law would not have any material utility or impact for these assets. For example, in order to transfer control of a password protected Word file that is stored in a hard drive, it would be necessary to hand over not only the password to the file but also the hard drive in which the file is recorded. If a person in control of the file were to send the file, for example as an email attachment, to another person who is given the password, that would not amount to a transfer of control. The file received would be an entirely new electronic record—albeit an exact copy of the material information. Moreover, as discussed in paragraph 6, control of the file would not impair rights existing under any applicable intellectual property laws. [One might view this circumstance as indicating that the scope of the Principles is overbroad. However, it is better characterized as merely an example of digital assets that would not normally be disposed of and consequently would not benefit from or involve the need for the legal regimes that the Principles contemplate. On the other hand, an attempt to narrow the definition of digital asset to exclude such digital assets might risk the exclusion of assets that would (or could) benefit from inclusion.]

(3) ‘~~Digital assets~~Principles law’ means any part of a State’s law relating to ~~digital assets~~ which falls within the scope of ~~these principles~~the Principles.

(4) ‘~~Other~~ law’ means a State’s law including ~~its digital assets~~to the extent it is not Principles law.

Commentary

15. Under Principle 1, these Principles cover private law issues relating to digital assets. Therefore, these Principles provide rules for issues such as the custody and transfer of, and the provision of security ~~interests~~rights in digital assets. Under this definition (3), all the rules provided by the Principles qualify as ‘~~digital assets~~Principles law’ once they have been adopted and implemented into a State’s law. For the avoidance of doubt, ‘Principles law’ thus also includes the Private International Law rules provided in Principle 5, once these rules have been implemented into a State’s law. Notably, these Principles take no position as to whether ~~[its rules]~~ ~~[they]~~ should be included in a State’s special law on digital assets, incorporated into more general laws, already follow from general laws, or are addressed by a combination of these approaches. On the technological, jurisdiction and organisational neutrality of these Principles, see more extensively above, under Introduction, Part II. Neutrality and the Relationship of Principles to National Law.

16. ~~'Digital-assetsPrinciples~~ law' may or may not already follow from general private law rules in a specific jurisdiction. ~~[If, in a specific jurisdiction, the law following from general private law rules is consistent with these Principles, these Principles consider such general private law rules as 'Principles law', but only to the extent they apply to digital assets as covered by these Principles.~~

~~16-17.~~ Pursuant to its principles of functionality and neutrality, these Principles do not prescribe a specific classification of digital assets. However, ~~the law should specify~~if, in a specific State, it is unclear, which (if any) of its existing rules or standards of general application ~~cover~~apply to digital assets ~~whenever controversial,~~ it is recommended this is clarified. This is specifically relevant where it concerns the acquisition and disposition of proprietary rights in digital assets. Notably, if a State's law includes classification of different types of property or assets which can be subject to proprietary rights which have different consequences, it is recommended that law ~~should~~specify which type or types of property digital assets are ~~(this could mean the introduction of a new type of asset).~~⁸ This may also mean, for instance, that States specify which (if any) of its existing rules or standards of general application govern the provision of security rights in digital assets. It does not mean that a State's law needs to list every rule or standard which applies to digital assets. Not only would this be far too complicated, it would also be unnecessary as these Principles are concerned with private law rules only, and proprietary rights in particular.~~]~~⁹ See also the commentary to Principle 3(1) below.

~~17-18.~~ Within a State's law, all law that is not '~~digital-assetsPrinciples~~ law' as defined here, is referred to as '~~the law~~ other ~~then digital-assets~~ law' in these Principles. '~~Digital-assetsPrinciples~~ law' AND 'other law' as defined here together form 'the law' ~~as defined in this definition (4).~~ [~~The law' also means the applicable State's law, possibly after, In a conflict of laws analysis as set out in Principle 5 has been performed.]~~specific case or instance.

⁸ ~~This text may need to be further aligned with the commentary to 3(1).~~

⁹ ~~This text may need to be further aligned with the commentary to 3(1).~~

Continued Issues Paper

16. With regard to Principle 2(1), a representative of the Netherlands from the Steering Committee has noted:

Possibly rethink the addition of 'or other intangible medium'. That contradicts the notion of 'electronic record', also there is presently no real alternative medium except human minds, which then need to be excluded in the comments (leading to confusing definitions). Incidentally, one could argue that certain forms of storage are not strictly speaking electronic: they are accessed through digital technology, but the storage itself may use methods that do not exactly rely on electrons (hard disks use magnetic fields, DVDs use physical changes in the material). Does storage in such an electronic but physical (tangible) medium count as an electronic (intangible?) medium or not?

17. In response to this, at DC9, it was suggested to only refer to 'electronic' medium, as this was an accepted and standard terminology, including in UNCITRAL instruments.

18. The removal of the word 'Controllable' from Principle 2(2) was agreed upon at WG5 (see paragraph 26 of the Report), given that the notion of control was already present in the latter part of the same sentence.

19. With regard to Principle 2(2), particularly in the Commentary, the WG may give consideration to including a sentence making it clear that 'control' in the control principle was exclusive control (discussion of rivalrousness).

20. The changes proposed in Principle 2(3) and 2(4) were originally discussed at WG5 (see paragraph 27, 31, and 32 of the Report). Following this, the proposal to consider whether the term "digital assets law" could be changed to "Principles law" was adopted at DC5. This was to reflect the consensus that the term 'Digital Assets Law' was misleading.

21. With regard to the other changes in Principles 2(3) and 2(4), at DC6, the drafting was revised in order to add more clarity. Some members of the DC have queried whether the words 'regarding private law issues governing digital assets' should be repeated in Principle 2(3), or if it should be mentioned in the Commentary.

22. At DC6, it was agreed to amend Principle 2(4) to add additional clarity by changing the terms 'the law' to 'other law' when referring laws outside of the Principles. Additionally, some of the examples in the Commentary have also been simplified and made easier to understand.

23. With regard to the changes to the Commentary, the changes to the Commentary for Principle 2(1), and 2(2) up until the deletion of Illustration 3 are only for adding additional clarity, as a representative of the Netherlands noted that one of the illustrations was very complicated.

24. With regard to the deletion of Illustration 3, this is to be aligned with the Principle on Linked Assets (Principle 4). The Commentary for that Principle includes such examples accordingly. These changes were made at DC7.

25. The changes made to (now) Illustration 3 and 4 are to provide further clarity to the reader with regard to the applicability of these Principles to items such as social media accounts, Word/Excel files, and files which may or may not be protected by passwords. These changes were made in response to several comments from the Steering Committee regarding the application of the Principles to such files and the use of real world platforms and data files. These changes were made at DC7.

26. Additionally, a representative of Turkey from the Steering Committee raised a question relating to physical control, where a non-passworded file was stored on a personal computer. The illustrations and the Commentary also cover this issue to a certain extent, such that the Principles law would have no material impact or utility for such assets.

27. With regard to the changes proposed to the Commentary for Principles 2(3) and 2(4), these are for the purposes of alignment with the new draft and to clarify, among other things, that States would not need to produce a list of every rule or standard which applies to digital assets within their jurisdictions. These changes were made at DC7. This particularly responds to a comment by a representative of the Netherlands in the Steering Committee which cautioned against an obligation to specify which national law rules apply (including classification).

28. With regard to some of the changes in the Commentary at Paragraph 17, these provide guidance to States on how to implement these Principles domestically, and references the types of practices some States have already adopted.

29. There remains a sentence in square brackets at the end of paragraph 14 in the Commentary. It is proposed to the WG that this sentence be removed. This is in line with comments from a representative of Uruguay from the Steering Committee which recommended to avoid issues of renvoi.

Principle 3: General principles

(1) ~~The law should provide that digital~~ **Digital** assets can be the subject of proprietary rights.

Commentary

1. Under Principle 1, these Principles cover private law issues and in particular proprietary rights relating to digital assets. This Principle 3(1) therefore provides, as a matter of principle, that the law (as defined under Principle 2(4)) should provide that digital assets can be the subject of proprietary rights. All rules provided in these Principles are built on this premiss. However, the question whether digital assets can be the subject of proprietary rights has been controversial in several jurisdictions. As courts in multiple high profile cases have considered that digital assets are the subject of proprietary rights, and several authoritative authors have expressed that digital assets *should* be the subject of proprietary rights,¹⁰ these Principles advise States to ~~end~~**increase** legal ~~uncertainty~~ on this issue and make explicit that digital assets can be the subject of proprietary rights. 'Proprietary rights' is defined in ~~p~~**P**inciple 3(2).

~~That States should provide that digital assets can be the subject of proprietary rights also means that if a State's~~**If a specific State** law includes classification of different types of property or assets which can be subject to proprietary rights which have different consequences, **and it is unclear how digital assets as defined in these Principles must be classified, it is recommended** that ~~law should~~**such States** specify which type or types of property digital assets are.

~~1. Moreover, from this Principle 3(1) it follows, for instance, that States should specify which (if any) of its existing rules or standards of general application govern the acquisition and disposition of proprietary rights in digital assets. Similarly, this applies in relation to the provision of security rights in digital assets. It does not mean that a State's law needs to list every rule or standard which applies to digital assets. Not only would this be far too complicated, it would also be unnecessary as these Principles are concerned with private law rules only, and proprietary rights in particular.~~

~~2. Finally, transitional provisions could specify whenever controversial which (if any) existing rules or standards do not apply to digital assets and which (if any) existing rules or standards are changed in relation to digital assets.~~

~~3.2. (2) In these Principles, references to proprietary rights include proprietary interests and rights with proprietary effects.~~

~~4.3.~~ 'Proprietary rights' in these Principles are used in a broad sense, in that 'proprietary rights' include both proprietary interests and rights with proprietary effects. This broad definition reflects the functional approach of these Principles which intend to cater for the largest variety of jurisdictions possible. Also, the definition of proprietary rights intends to express that persons can have rights or interests in digital assets, which rights or interests can be asserted against third parties, ie against persons that are not necessarily contractual parties. This may be particularly relevant in the context of insolvency, where a liquidator or insolvency administrator might assert rights or interests in digital assets on behalf of the insolvent debtor's estate and/or its creditors against third parties, and vice-versa.

~~(3) The~~**(2) Principles law takes precedence over other than law to the extent that they conflict.**

¹⁰ [sources to be added]

4. These Principles provide specific rules for the holding, transfer and use of digital assets~~law continues to~~, taking into account the specific nature of this asset class. This means these rules may supplement or derogate from both more general, and specific State laws. To give the rules of these Principles full effect, these Principles should take precedence over both more general, and specific State laws whenever they conflict. Consequently, once they have been adopted and implemented into a State's law, these Principles (by then 'Principles law' as defined in Principle 2(3)) must take precedence over other law (as defined in Principle 2(4)).

5. As already stated above, these Principles take no position as to whether its rules should be included in a State's special law on digital assets, incorporated into more general laws, already follow from general laws, or are addressed by a combination of these approaches. However, whenever it is unclear whether Principles law (as defined) takes precedence over other law (as defined), it is advisable to make this explicit. See also Principle 2.

6. Finally, transitional provisions could specify – whenever unclear – which (if any) existing rules or standards do not apply to digital assets and which (if any) existing rules or standards are changed in relation to digital assets.

(3) Except as displaced by these Principles, other law applies to all issues not dealt with in these Principles, including

- (a) **whether a person has a proprietary right in a digital asset;**
- (b) **whether a ~~person has validly transferred a~~ proprietary right in a digital asset has been validly transferred to another person;**
- (c) **whether a ~~person has validly created a~~ security right in a digital asset has been validly created;**
- (d) **the rights as between a transferor and transferee of a digital asset;**
- (e) **the rights as between a grantor of a security right in a digital asset and the relevant secured creditor**
- (f) **the legal consequences of third party effectiveness of a transfer of digital assets; and**
- (g) **the requirements for, and legal consequences of, third party effectiveness of a security right in a digital asset.**

Commentary

~~5.7.~~ This Principle 3(3) makes explicit that other law, i.e. all law within a given State that is not '~~digital assets~~Principles law' as defined in Principle 2(3), continues to apply to digital assets. For this purpose, ~~this~~ Principle 3(3) lists several examples of issues of property law, but also of contract law, that may continue to be regulated by a State's other law, because these Principles do not cover those issues, nor do they intend to change or derogate from that other law. The list is not intended to be exhaustive or limitative. It is reiterated that, first, these Principles cover only private law issues relating to digital assets, so that they do not cover rules that are to be enforced by public authorities which in many jurisdictions would be called 'regulation' or 'regulatory law'. Moreover, these Principles intend to only regulate a specific area of private law, and there are many issues of private law which are not addressed by the Principles. These issues concern, for instance, rules of private law relating to intellectual property or consumer protection. As a matter of principle, these areas of law are not addressed by these Principles, and national intellectual property and consumer protection laws therefore remain unimpaired by them. Finally, there are several issues of property and contract law that these Principles do not cover, and this Principle 3(3) lists important examples those issues. Strictly speaking, 'Except as displaced by these Principles' is redundant, because 'other law' (as

defined), is, by definition, law that is not covered by these Principles. It has been for the avoidance of any doubt that Principle 3(3) says that 'except as displaced by these Principles', other law continues to apply. It is not meant to say that a specific State law continues to apply only to the extent these Principles (as contrasted with Principles law) explicitly displace such State law.

~~6-8.~~ The examples in ~~this~~ Principle 3(3) of issues that continue to be regulated by other law, can be categorized as follows. First, Principle 3(3)(a) concerns the static situation in which it must be determined whether a person has a proprietary right in a digital asset. Pursuant to ~~this~~ Principle 3(3)(a), the requirements for a (valid) right or interest in a digital asset that can be asserted against third parties, continues to be a matter of other law. Therefore, and by way of example, whether a person holds a valid right of ownership in certain digital assets, is, as a matter of principle, not regulated by these Principles.

~~7-9.~~ Second, Principles 3(3)(b) and (c) concern dynamic situations of acquisition and disposition of digital assets from the perspective of the transferor and security right provider, respectively. If the question arises whether a person has validly transferred a proprietary right, or validly created a security right in a digital asset, ~~these~~ Principles 3(3)(b) and (c) make it clear that the requirements for a (valid) transfer and creation of a security interestright continue to be, as a matter of principle, a matter of other law. ~~{However, these Principles do provide for specific issrules regarding the transfer of, and creationthird-party effectiveness (perfection) of a security interestright in digital assets: these provisions are then'.~~ Whenever it is unclear whether existing rules or standards of general application apply to digital assets law', which takes precedence over other law.} ~~[These issues are then covered by the, and whenever Principles, which is considered 'digital assets law' and takes precedence over 'other law'.~~ law derogates from other law, it is recommended State law makes this explicit. Principle ~~16(2), for instance,~~9 provides that ~~a State's law should provide distinct rules in relation to creation of a security right and effectiveness against third parties 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.}~~an innocent acquirer takes free from conflicting proprietary rights.

~~8-10.~~ Principles 3(3)(d) and (e) make explicit that the relationships between a transferor and transferee, and between a providergrantor of a security right and the relevant secured creditor, respectively, continue to be a matter of other law and are not, as a matter of principle, regulated by these Principles. In several situations and jurisdictions, these relationships are characterised as primarily contractual in nature. Principles 3(3)(d) and (e) provide that the rights between a transferor of digital assets and the transferee, and a providergrantor of a security right in digital assets and the secured creditor, are left to be dealt with by other law, whatever the qualification of the relationships between those parties.

~~9-11.~~ As explained above, Principles 3(3)(d) and (e) concern the (contractual) relationships between a transferor and transferee, and between a providergrantor of a security right and the relevant secured creditor, respectively. These provisions thus concern *inter se* relationships, i.e. relationships between (contracting) parties. Principles 3(3)(f) and (g), on the other hand, concern *erga omnes* relationships, i.e. the relationships with third parties. Pursuant to these Principles 3(3)(f) and (g), whether a transfer and a creation of a security interestright, respectively, can be asserted against third parties, continue to be, as a matter of principle, a matter of other law. In several jurisdictions, the 'assertability' of a right or interest against third parties follows from the concept of 'effectiveness'. ~~These~~ Principles 3(3)(f) and (g) provide that, whatever the dogmatic context, the requirements for such effectiveness or assertability continue to be, as a matter of principle, a matter of other law. However, these Principles do provide for specific issrules regarding the effects of proprietary rights or interest in digital assets. ~~{These provisions are then'As also stated above, whenever it is unclear whether existing rules or standards of general application apply to digital assets law', which takes precedence over other law.}~~ Whenever it is unclear whether existing rules or standards of general application apply to digital assets law', which takes precedence over other law.} ~~[These issues are then covered by the, and whenever Principles, which is considered 'digital assets law' and takes precedence over 'other law'.~~ law derogates from other law (as defined), it is recommended State law makes this explicit. In that

[vein](#), Principle 17, for instance, provides that a State's law ~~might~~[may](#) provide distinct ~~rules-in~~[relation](#)~~methods~~ to [achieve](#) the effectiveness of a security right in digital assets.

Continued Issues Paper

30. For Principle 3(2), consideration was given at DC7 to including the terms ‘...other law relating to private law matters ...’. However, this was considered to be too narrow and later removed from the draft.

31. Principle 3(3) detailing the relationship between principles law and other law was introduced during DC6. The Commentary regarding Principles’ law taking precedence over other law has been expanded, while the Principles were given a more succinct wording. Additional parts of Principle 3(3) have been redrafted in a more passive style for consistency and to suit the nature of the Principles document. An additional line in the Commentary for Principle 3(3) now addresses that in the case of an innocent acquirer, the Principles would apply.

32. On this Principle, a representative of Japan from the Steering Committee commented as follows:

Principle 3 does not have clear definition or the list of proprietary issues that the Principle intend to cover, but only has the list of issues that will not be covered by the Principle. The Commentary refers Principle 3(2) as the definition of “proprietary rights”, but Principle 3(2) seems not clear enough as a definition (because it does not specify what proprietary interests and rights with proprietary effects means and because it is still unclear what would be included in proprietary rights other than proprietary interests and rights with proprietary effects. If the proprietary rights in the Principles mean the same rights that would be conferred on the possessor or owner of a tangible object with a similar function under the laws of the country concerned, then it would be better to specifically state so. Alternatively, if you want to clarify the content of some specific proprietary rights under the Principles regardless of the laws of the countries concerned, it seems better to not only list the matters to which the Principles do not apply, but also the matters to which the Principles do apply, thereby further clarifying the content of the proprietary rights as contemplated by the Principles (as Geneva Convention).

Regarding the Principle 3(3), it is my impression that too many proprietary law issues are not covered by the Principles, and it is unclear to me from the explanation in the Commentary why such very narrow scope of the Principles is appropriate. For example, issues as listed in (a) (b) (c) must closely relate to the effectiveness of collateralization and the status of holders of digital assets in insolvency, both of which are within the scope of the Principles. It is not clear to me why such distinction was chosen.

33. To address this, several insertions have been made to the Commentary to further explain the scope of the Principles.

34. The parts of the Commentary relating to transitional rules has been moved. The usefulness of this will depend upon how a State decides to implement these Principles domestically.

35. Additionally, consideration is also being given to defining the term ‘proprietary’ as part of this Section.

Principle 4: Digital Assets 'Linked' to Linked assets

Other Assets

~~(1) — Where law applies to determine the existence of, requirements for, and legal effect of any link between a digital asset, or any related system protocols or documentation, appears to confer a right to and another asset, which can be whether the other asset is tangible or intangible ('the other asset'), the legal effect (if any) is a matter for the law, [other than the digital asset law,] [and is not addressed in these principles].~~

~~(2) — The law specifies the requirements to be met, including as regards the form and content of the information to be provided, for any legal effect to occur.~~

Alternative formulation for discussion:

~~The requirements to be met for any legal effect to occur (including as regards the form and content of the information to be provided) are a matter for the law to specify.~~

Commentary

10. — The purpose of this principle is to identify the limit of the principles as regards digital assets 'linked' to other assets [*Note: these types of digital assets will be already referred to in the context of commentary on the definitions (Principle 2)*].

11. — The principle makes clear that the legal effect of the link (if any) is not addressed in these principles, in particular because: (i) the nature of the link may vary from case to case depending on the facts and on the law, and (ii) the issue of proprietary rights in the 'other asset' is a matter that is to be determined in accordance with the law applicable to that asset (paragraph 1). 'Legal effect' means any type of legal effect, including, most importantly, questions as to the enforceability of acquisitions and dispositions, including their enforceability in insolvency. [The principle confirms that 'the law' is a State's law other than the 'digital assets law' (defined Principle 2(3)).]

12. — The principle underlines the importance of [jurisdictions][States] developing rules to specify the nature of relevant information required to be made available for a legal effect to materialise, in addition to all other requirements the law may set (paragraph 2). This is important to ensure that there is a minimum evidentiary basis on which the intentions and understanding of parties can be identified.

13. — In line with a technology neutral approach, the principle recognises that the information giving the appearance of conferral of a right may be encoded in the digital asset and/or may appear in any related system protocols or other documentation, e.g. a white paper. The use of the word 'appears' in paragraph 1 reflects the fact that that there may be scenarios where the code or documentation states or implies the existence of a link but ultimately whether this link exists, and what its effect may be (if any), is a matter for the law.

14. — The reference to 'a right to another asset' in paragraph 1 has a broad meaning and means rights in relation to the 'other asset' itself. What is not meant are rights to take action, e.g. against an issuer for non-performance of an obligation.

15. — The principle does not assume any limitation on what the nature of the 'other asset' may or may not be. As such, 'other assets' is to be interpreted broadly and may be intangibles or tangibles.

16. — The principle does not address the question of which State's law (State A, B, C etc) is applicable (that question is addressed in Principle 5).

Examples of 'linked' assets:

~~As illustration of the fact the link between a digital asset and another asset may operate in various ways, depending on the intention on the parties to the transaction and the effect given to it by the [general] law, [4] illustrative examples follow:~~

1. As provided in Principle 4, a digital asset may appear to be linked to another asset or assets. It is a matter for the other law of the State, including its regulatory law, to determine whether any such link is sufficiently established and to determine what, if any, the legal effect of the link may be.

2. As examples of possible links, a White Paper may contemplate that a transfer of the digital asset should have some effect on the rights of its holder in relation to the other asset or against a person who issued it. A transfer of the digital asset may have the effect of transferring rights in the other asset. In other cases, the effect of the link may be that the value of the other asset determines the value of the digital asset.

3. The "other asset" referred to in Principle 4 may be tangible or intangible, and may also include another digital asset. The other asset is one which exists contemporaneously with, but separately from, the digital asset. It does not include a "resulting digital asset", within the meaning of Principle 6(2), which only comes into existence to give effect to some change in the control of an original digital asset.

4. The operation of linked assets in Principle 4 depends on two distinct questions: (1) whether there is any link at all between the digital asset and the other asset; and (2) whether the link has a legal effect on the parties' rights in relation to the other asset.

5. Whether the link is proved to exist is primarily a question of fact, although the regulatory law or other law of the State may define minimum standards of certainty for recognising the link. A link which failed to reach those general standards would be ineffective to affect any rights of the parties in relation to the other asset. Subject to these general rules, the existence of any link depends on all the circumstances of the case and the intentions of the parties who create the digital asset. The link may be apparent from the coding of the digital asset or from any related system protocols applying to it. It may also be apparent from any published documentation relating to the digital asset or the other asset, such as a White Paper or the terms of issue of applying to them.

6. Even when the existence of the link between the digital and the other asset is satisfactorily proved, its legal effect depends on the other law. 'Legal effect' is to be understood broadly. It includes, most importantly, the effect of any transaction with the digital asset on the parties' rights in relation to the other asset, and the effect of those transactions in insolvency. The legal effect of the link may also include the effect of any transaction with the digital asset on any contractual rights between the holder of the digital asset and the holder of the other asset.

7. The parties who issue or transact with the digital asset cannot confer any greater legal effect on the link than the other law would allow. In this way, transactions with a linked digital asset do not necessarily have the same legal effect as transactions with conventional securities recorded in a legally-constituted registry system. In such a system, the alteration of the register causes a change in the parties' rights to the securities recorded on it. The reason is that a legal rule creates a legal link between the state of the register and the state of legal rights in relation to the securities. By contrast, a change in recorded holding of a digital asset is legally neutral in relation to the other asset unless some other law makes the link between them legally effective.

8. The legal effect may be determined by existing rules of other law, or a state may provide for it in special rules developed for linked assets. The other law may recognise the existence of the link without also recognising that a disposition of the digital asset has any legal effect at all on the parties' rights in relation to the other asset. A separate legal act maybe required to change the parties' rights to the other asset.

9. The other law of a state may determine that the benefit of any innocent acquisition rule applied to a digital asset in accordance with Principle 9 should also apply to the other asset linked to it. In the usual way, however, the simple proof of the link between the digital asset and the other asset would not necessarily mean that the holder of the other asset took the benefit of the innocent acquisition rule. The other law of the state would need to provide for this result.

10. As illustrations of the different legal effects of a link between the digital asset and the other asset, [6] examples follow:

~~17.~~11. **Illustration 1:** The general rules of other law already in force may recognise that apply to the parties' transaction with the digital asset and determine the legal effect on the blockchain ledger is legally effective to change the state of proprietary rights in the other asset off the ledger linked to it.

~~18.~~12. For example, a system may be established for trading quantities of tokenised gold [e.g. PAX Gold]. An investor who buys may hold a digital token from the issuer acquires which evidences a proprietary right in a fractional share of specifically identified gold. Whether a sale and transfer of the token may pass passes the seller's proprietary right in the gold to the buyer. The link between the token and the gold is legally effective if the general law treats the depends on the other rules of sales law that apply to gold in the applicable legal system. In some legal systems, the other law may treat the parties' dealings with the digital token as the outward expression of their intention to transfer the proprietary right in the gold. The proprietary right in the gold would pass to the buyer of the token. However, even if the other law treats the dealing with the token as effective to transfer the proprietary right in the gold, it may not preclude the parties from dealing with the gold separately from the digital token. The effect may be that proprietary rights in the gold and the token become de-synchronised. In other legal systems, the seller may be required to deliver the gold to the buyer in order pass the proprietary right in it. In such a legal system, a sale and transfer of the token would not pass the proprietary right in the gold. It might, however, be evidence of a completed contractual right to enforce a transfer of the gold against the seller.

~~19.~~13. **Illustration 2:** A State may choose to enact special legislation to make the link between the token and the other asset legally effective to transfer rights in the other asset.

~~20.~~14. For example, a company may raise finance from investors by issuing debt securities on a blockchain ledger. Each investor holds a transferable digital token representing their security claim against the debt issuer. It purports to give the investor a right to payment by the debt issuer. When the token is transferred on the ledger, the transferee acquires the proprietary right in against the security debt issuer. The company which issued the debt security gets a good discharge if it pays the current holder of the token. Special legislation may be needed to effect this result if it cannot be achieved, for example, by the sState's existing general other law of assignment, novation or securities transfer.

~~21.~~15. **Illustration 3:** The precise legal effect of any link between the digital asset and the other another asset may depend as much on ascertaining the parties' intentions from any system coding, protocols and documentation as it does from the operation of the general other law. Thus, the terms of a White Paper accompanying the issue of digital asset may be relevant to inferring the nature and value of the legal right, if any, that the holder of the digital asset was intended to have in relation the other asset.

~~22.~~16. For example, an issue of stable coins may take the form of transferable tokens which are denominated in the units of a fiat currency, such as USD [e.g. the Tether stable coin]. For each USD unit of stable coins created, the issuer creates a 1:1 reserve of liquid assets denominated in USD. The reserve is held by a custodian, separately from the issuer's own assets. The White Paper may provide that any holder of the stable coin is entitled to re-sell it to the issuer at par value in USD.

The effect of this right to resale is to stabilise the transfer value of the coin as it circulates in payment transactions.

~~23.17.~~ The legal effect of transferring the stable coin and any rights it may appear to confer against the issuer may depend as much on the other law of assignment or novation of contractual rights as it does on the terms of the White Paper. The terms of the White Paper may show that each holder of the coin was primarily intended to have a contractual right against the issuer. ~~It~~ The transfer of the stable coin may operate as an assignment or novation of that right. Even if the holder of the token had a proprietary right in the stable coin, it may be apparent from the other law or from the terms of the White Paper that the holder would, ~~however,~~ not also have a proprietary right in the other assets held in the reserve. It would be for the insolvency law rules of the ~~relevant state~~ other law to determine how, if at all, this right might take priority over any other claims ~~of general creditors~~ of enforceable against the issuer.

~~24.18.~~ **Illustration 4:** Digital assets may be used to create transferable portions of value derived from other assets which exist off the blockchain. The ~~Even when the link between the digital assets and the other assets is clear, the~~ precise ascertainment effect of the holders' rights ~~may~~ will be determined ~~—and limited—~~ by the ~~general~~ other law of the state. The parties' intention to link the assets cannot override the other law that applies to those assets.

~~25.19.~~ For example, an issuer may sell digital assets that purport to give the holder a claim in relation to real estate. The assets are transferable on a blockchain ledger. On closer analysis, most tokenised real estate actually involves the establishment of a company to which ownership of the real estate is transferred. The shares in the company are then 'tokenised' and made transferable on the ledger. The transfer of the token may not be sufficient in law to transfer the shares in the company or any proprietary interest in the real estate. These may be questions for the system of other law where the company is registered, or the real estate is located. The relevance of the digital asset is to illustrate: (i) the 'chain' of ownership legal relations between the holder and the shares and the real estate; and (ii) steps that may need to be taken by the acquirer of the token ~~(and depending on the law and administrative practices of the jurisdiction concerned)~~ to update a company register; or update a register of real estate.

~~26.20.~~ This illustration shows that the mere fact of the transfer of the token from one person to another may not ~~be enough by itself to~~ perfect the transfer of ownership of shares or the real estate. ~~It~~ Nor may the existence of one person's control over the token be sufficient to prevent the transfer of shares or the real estate from ~~one person to another~~ being transferred independently of any dealing with the token.

~~21.~~ [~~Note further examples~~ States could, if they wish, require, as a matter of regulation, disclosure of information as to ~~be inserted e.g. tokenised bonds: here, the issuing document specifies~~ any purported link between the digital asset and the other asset, and, if desired, could specify the form that ~~the principle and coupon are owed~~ that disclosure must take.]

~~22.~~ **Illustration 5:** One digital asset may be linked to another digital asset and the legal link between them would depend on the effect of any legal relations between the holders of the two assets.

~~23.~~ For example, an issuer may create a digital asset which is a "wrapped" version of another digital asset on a different protocol. Like the "stable coin" in illustration 3, only ~~to one~~ "wrapped" digital asset would be created for every other digital asset on the other protocol. The White Paper may provide that the holder of the wrapped digital asset ~~is~~ entitled to redeem the other digital asset. In some cases ~~return,~~ the holder's wrapped digital asset would be "burned". The effect of this ~~will be~~ supplemented by a provision that the debt obligation cannot be ~~1:1~~ relationship is that the value of the wrapped digital asset should correspond to the value of the other digital asset. When the wrapped digital asset is ~~transferred to a person unless the,~~ the transferee should receive the same value as

if the other digital asset had been transferred between them. The rights of the holder of the wrapped asset in relation to the other asset would depend on the legal effect of the link between them. The terms of a contract between the issuer and holder of the wrapped digital asset would determine if the holder had a right to regain control of the other digital asset and have the wrapped asset was “burned” at that point.

24. **Illustration 6:** The other law of a state may recognise a good faith acquisition rule in relation to the other asset linked to the digital asset. The effect may be that both the digital asset and the other asset would benefit from a good faith acquisition rule.

~~27-25.~~ For example, as in illustration 1 above, a system may be established for trading quantities of tokenised gold and an investor may hold a digital token ~~is~~ which evidences a proprietary right in a fractional share of specifically identified gold. A hacker may unlawfully obtain control of the token and transfer it by sale to an innocent buyer. Under Principle 9, the buyer would acquire a proprietary interest in the token which was free from the claims of the original investor who once held the token. It would be, however, for the other sales law of the state to determine whether the innocent buyer would also ~~transferred~~ acquire a proprietary right in the share of the gold and take it free of the original investor’s claims.

Continued Issues Paper

36. Significant consideration was given by the Drafting Committee to including this Principle as part of Principle 3(3). During DC6, it was decided that a stand-alone linked assets provision should be introduced into the scope of General Principles contained in Principle 3. For DC7 and DC8, there were two alternative provisions on linked assets: a short Principle 3(3)(h) or a more extensive Principle 3(4), containing further illustrations. After DC8, has was redrafted with a general explanation and clarification of the innocent acquisition rule, and emphasis that the effect of the linkage depended on the national law of each State, and further illustrations with positive and negative examples being expected to be introduced. The substance of the provision, i.e., that the legal significance of the link is a matter for the other law of States to regulate is reflected in both versions of the provision.

37. Additional guidance for States with regard to requirements for linked assets is included in the Commentary for the Principle. This includes mention on possible disclosure requirements.

38. During DC9 it was agreed that the alternative, more extensive version of the principle was preferable, allowing for more extensive commentary. This was also in light of several comments on this from the Steering Committee which expressed some confusion with regard to the issue of linked assets.

39. For this Principle, a representative of the United States from the Steering Committee commented as follows:

We agree generally that, the extent to which another asset is linked to a digital asset, other law should determine the effect of that link. We wonder, though, whether the Principles might deal with certain payment rights linked to the digital asset so that the payment rights have the same proprietary protections as the digital asset. Doing would permit, for example, electronic promissory notes and bills of exchange, helpful in trade finance. Perhaps this point is already addressed by the law dealing with transferable records.

40. Some additional commentary has been added to address this matter.

41. A representative of the Netherlands from the Steering Committee commented on this Principle as follows:

Given the above considerations, the issue is not whether there is an appearance of linkage but whether there is a legal basis for effective linkage. This is needed to distinguish from meaningless 'registrations' such as the Star register (<https://starregister.org/>). Such a legal basis should – in the Dutch view – principally be found in specific statutes, given the large variety of consequences that these links can have, and the importance of legal certainty on who is or is not owner in case of errors or fraud in the registration, as well as the need for corrections after annulment of contracts.

Where the issue is linkage to intangible items that do not have direct social consequences, a relaxed view is conceivable, as in the case of NFTs. The reason is that those are self-contained systems that need to be enforced within their own domain, while the registry of tangible immovables needs to be reliable for reasons of public policy.

42. It is noted that the Commentary already addresses these issues and has been expanded accordingly.

43. A representative of Luxembourg from the Steering Committee raised the following points with regard to this Principle:

It would be helpful if Principle 4(1) could be clarified in three respects:

(i) With 'right to another asset', does it mean only a right to the entire asset (like title to a house) or also right to a share of the underlying asset (like a share in a limited company)? One assumes both but worth clarifying in examples.

(ii) Does the principle at all seek to cover digital assets that confer a right to another digital asset? If yes, is it then still natural to interpret 'the law' as 'other than the digital asset law'?

(iii) Except from pure non-stable cryptocurrencies like Bitcoin, all real world examples of "true" crypto-assets confer a right to another asset in some way; yet, the overly broad definition of the Principles may also capture concepts beyond that. For instance, utility tokens confer a right to a claim on future (digital) goods or services. Depending on how you interpret that the 'legal effect' of such arrangements is a 'matter for the law' ... 'and not addressed in these Principles', you may argue that the entire set of Principles do not apply to the vast majority of digital assets, which I assume is not the intention. Hence, I encourage to clarify Principle 4(1).

More generally, I wonder if Principle 4 relates more to the scope of the overall Principles – I suggest to move and integrate in the overall Principles accordingly.

44. The Commentary has been expanded to explain these points further. It is also noted that only the link between the assets is not covered by the Principles, whereas the relationship is generally explained in the Commentary and in other parts of the draft.

45. The changes made to Illustration 2 were the result of comments from a representative of Switzerland from the Steering Committee who noted that rather than 'representing their security', it should say 'representing their claim against the debt issuer'. This was supported by the Drafting Committee.

SECTION II: PRIVATE INTERNATIONAL LAW

Principle 5 – Conflict of ~~L~~aws ¹¹

~~1) — General principle~~

~~a) (1) Subject to paragraph (2), proprietary issues in respect of a digital asset are governed by:~~

~~(a) the domestic law of the State (excluding that State's conflict of laws rules) expressly specified in the digital asset as the law applicable to such issues;~~

~~(b) If subparagraph (a) does not apply, the domestic law of the State (excluding that State's conflict of laws rules) expressly specified in the system or platform on which the digital asset is recorded as the law applicable to such issues;~~

~~(c) If neither subparagraph (a) nor subparagraph (b) applies:~~

~~(i) these Principles; and~~

~~(ii) to the extent not addressed by these Principles, the law applicable by virtue of the rules of private international law of the forum.~~

~~(2) In the interpretation and application of paragraph (1), regard is to be had to the following:~~

~~(a) Proprietary ~~questions~~issues in respect of digital assets, and in particular their acquisition and disposition, are always a matter of ~~the law of a State~~.~~

~~b) The digital assets law should include the following rule determining the law applicable to proprietary questions in respect of digital assets:~~

~~2) — Determination (b) In determining whether the applicable law is specified in a digital asset, or in a system or platform on which the digital asset is recorded, consideration should be given to records attached to or associated with the digital asset or the system or platform if such records are readily available for review by persons dealing with the relevant digital asset.~~

~~(c) By disposing of, acquiring, or otherwise dealing with a digital asset a person is deemed to consent to the law applicable under paragraph (1)(a) and (b).~~

~~(d) Unless an express specification of the applicable law~~

~~The or the applicable rules of private international law applicable to proprietary questions in digital assets~~

~~a) — The otherwise provide, the law applicable to propriety questions in respect of digital assets is identical for under paragraph (1) applies to all digital assets of the same description.~~

¹¹ [We recognise that a conflict-of-laws rule will always be imperfect. These principles' aim is therefore to improve the clarity and legal certainty surrounding the issue of conflict-of-laws to the largest possible extent.]

~~b) — The applicable law is to be chosen at the moment of the first issuance of assets being of a specific description. The digital asset law should take measures incentivising such choice.~~

~~c) — The choice of the applicable law can be included in the code or can be manifested in accompanying documentation. The digital asset law determines the relevant requirements.~~

~~d) — The digital asset law can restrict the choice of applicable law; in particular, regulated parties can be directed to transact in digital assets only to the extent that the proprietary aspects in respect of these assets are governed by a specific law or by a law to be chosen from a specific group of laws. A choice of law not compliant with the restriction is not valid the time that a digital asset is first issued or created.~~

~~(e) If no valid choice has been made, the law applicable to proprietary aspects of a digital asset is the law that generally applies to the relevant [network] [asset or the system] or platform on which the relevant digital assets are created.~~

~~f) — If no law has been chosen in respect of asset is recorded expressly specifies the applicable law effective from a time after the time that the relevant [network] [system] digital asset is first issued or created, rights and interests in the law of digital asset that are established before the State to which express specification becomes effective are not affected by the [network] [system] has the strongest factual connection applies, in particular in cases in which the network operator is resident, incorporated or regulated or has otherwise a clear factual connection to a specific State specification.~~

(3) Recognition in insolvency

Notwithstanding the opening of an insolvency proceeding, and subject to paragraph (4), the law applicable in accordance with ~~the previous rules~~ this Principle governs all proprietary aspects in respect of digital assets with regard to any event that has occurred before the opening of that insolvency proceeding.

Commentary

~~1. The purpose~~ (4) Paragraph (3) does not affect the application of any substantive or procedural rule of law applicable by virtue of an insolvency proceeding, such as any rule relating to:

(a) the ranking of categories of claims;

(b) the avoidance of a transaction as a preference or a transfer in fraud of creditors; or

(c) the enforcement of rights to property that is under the control or supervision of the insolvency administrator.

Commentary

1. Principle 5 addresses the applicable law for proprietary issues that are covered by the Principles. However, it may be expected that a state (or tribunal) that adopts Principle 5 may extend its application to proprietary (and other) issues beyond those that the Principles address.

2. This Principle recognises that the usual connecting factors for choice-of-law rules (e.g., the location of persons, offices, activity, or assets) have no useful role to play in the context of the law applicable to proprietary issues relating to digital assets. Indeed, adoption of such factors would be incoherent and futile. Instead, the approach of this Principle is to provide an incentive for those who create new digital assets or govern existing systems for digital assets to specify the applicable law

in or in association with the digital asset itself or the relevant system or platform. This approach would accommodate the special characteristics of digital assets and the proprietary questions concerning digital assets that may arise.

3. Paragraph (1) provides a 'waterfall' of factors for the determination of the applicable law. Under paragraph (1)(a) ~~is to make sure that the~~, the applicable law is the law of the State specified in the digital asset itself. If subparagraph (a) does not apply, the applicable law is that of the State specified in the system or platform in which the digital asset is recorded. Those choice-of-law rules are appropriately based on party autonomy, because Paragraph 2(c) deems every person dealing with a digital asset to consent to the choice of law rules in paragraph (1). Persons who could be affected by a determination of a proprietary issue would be deemed to have consented. This reliance on party autonomy is consistent with the Hague Conference Principles on Choice of Law in International Commercial Contracts ('Hague Conference Principles').

4. At the bottom of the 'waterfall', in the absence of a specification made in the digital asset or the system or platform as contemplated by paragraphs (1)(a) and (b), under paragraph (c) the forum would be required to apply to proprietary questions in respect of a digital asset the UNIDROIT Principles and, as to the extent not addressed by the Principles, the law otherwise applicable under the private international law rules of the forum. This approach draws on Article 3 of the Hague Conference Principles. Article 3 offers a 'novel solution[]' that 'allows the parties to choose not only the law of a State but also "rules of law", emanating from non-State sources.' Hague Conference, Principles, ¶ 1.18; see also *ibid.* ¶¶ 2.5, 3.1-3.12. Because these Principles are generally accepted on an international level as a neutral and balanced set of rules, their application at the bottom of the waterfall is appropriate. Article 3 confirms that such a set of rules can provide the applicable law in a conflicts of law situation.

5. It would also be possible for a digital asset, or a system or platform, to specify that the UNIDROIT Principles (supplemented where necessary by the law applicable by virtue of the rules of private international law of the forum) would be the law applicable to proprietary issues. [Accordingly, paragraph (1) might usefully be revised to refer explicitly to such a specification of these Principles in a digital asset or a system or platform.]

6. By placing these Principles at the bottom of the waterfall, Principle 5 provides an innovative means of permitting a forum to adopt the Principles for persons and matters subject to its jurisdiction when paragraphs (1)(a) and (b) do not apply. The adoption of Principle 5 would accommodate the wish of a forum to adopt the Principles in such situations. In particular, the forum would apply the Principles even when the substantive law of a forum state itself otherwise would apply, without the potential delay and complexity in making substantial revisions of otherwise applicable local private law. Indeed, a forum state might choose this approach either as its primary means of adopting the Principles or as an interim approach. Of course, if the relevant digital asset or system specified the substantive law of the forum state (which would thereby apply under paragraph (1)(a) or (b)) it is reasonable to assume that the forum state would have adopted acceptable substantive rules such as those exemplified by these Principles.

7. Paragraph (2) provides additional guidance on the interpretation and application of paragraph (1). Paragraph 2(a) confirms that law applies to a proprietary issue regardless of whether (a) the participants in the relevant network refute the application of any law and exclusively want to rely on code, or (b) the application of the law is said to be too complex or to produce unclear outcomes or to disrupt the functioning of the network, as a consequence of the nature of the technology, or of the international character of the network. ~~As presently drafted, 'law' is a State's law (as defined in Principle 2(4)), but it could also be the UNIDROIT Principles if the text in square brackets is omitted.~~

2. ~~Paragraph (2) deals with the determination of the law applicable to proprietary questions in relation to digital assets. There are three important aspects: (a) the law is chosen uniformly for all assets of a specific issue, (b) it should be a visible (not secret) choice, (c) assets of different issues~~

~~can be stored and transacted on the same system, cf Ethereum. The law of the asset and the law of the system may be the same or it may be different.~~

~~3. — The default rule set out in paragraph 2(a) to (d) is that the applicable law is chosen as set out in sub-paragraph (b). The reference to assets ‘of the same description’ in sub-paragraph 2(a) is to assets of the same issue, that is, assets that in a tradition setting would have the same ISIN number.~~

8. Principle 5 concerns only choice-of-law issues and does not address the question of the jurisdiction of any tribunal over a party or the subject matter at issue.

9. Paragraph (3) makes it clear that in an insolvency proceeding Principle 5 should be applied to proprietary questions in respect of a digital asset. Paragraph (4) provides the usual exceptions that defer to the applicable insolvency laws.

Continued Issues Paper:

46. Amended Principle 5 on Conflict of Laws is a result of discussions which took place at WG5 and intersessional work undertaken at DC5 and DC7.

47. While separation of the Principle into several parts was considered in detail during the Working Group meeting and DC5, preference was given to keeping it as a single piece. At WG5, the Working Group agreed on the overall waterfall structure of the redrafted Principle on conflict of laws but raised concerns regarding a number of points, including: (a) connecting factors as relating to location, and any possible alternatives to location in the context of DLT operation; (b) Scoping of the Conflict of Laws Principle, particularly its interaction with other law governing insolvency; (c) The coverage of different types of digital assets by these Principles (i.e. would certain assets be excluded by these Principles); (d) How issuers could be incentivised to make a choice of law for digital assets of the same issue; (e) The inclusion of the choice of applicable law in the code of the digital assets as was mentioned in paragraph 5(2)(c) of the previous draft; and (f) Whether the sequence of the waterfall structure should be reversed or rearranged.

48. It was agreed that the scope of the Principle should not be strictly limited to the proprietary questions and allow for some degree of flexibility as may be preferred by a state or a tribunal in question.

49. At DC5, the earlier waterfall structure of connecting factors was preserved prioritising the law specified in the digital asset itself over the law specified for the system or platform on which the digital asset is recorded. However, the 'bottom' of the waterfall was added comprising the present Principles and, to the extent not covered by these Principles, the law applicable by virtue of the private international law rules of the forum. This was made to address concerns raised during WG5 that a lot of digital assets would 'fall through' the proposed connecting factors without determining the applicable law.

50. It was noted that the underlying rationale of the Principle was that there should be a choice of law, and when there was no choice of law there was a fallback mechanism with two parts: the first part determined the applicable law, or where there was no connecting factor, there was the second part which was the bottom of the waterfall. Despite a difference in appearance of the revised Principle, the underlying logical remained the same.

51. DC7 further discussed and agreed on the revised draft of Principle 5, including the 'bottom' of the waterfall. With regard to the scope of the Principle, the Drafting Committee discussed and agreed that it ought not be strictly limited to the proprietary questions and allow for some degree of flexibility as may be preferred by a State or a tribunal in question. This was reflected in the Commentary at para. 1. As further explained in the Commentary, the proposed choice-of-law rules underlined the reliance on party autonomy which was consistent with the Hague Conference Principles on Choice of Law in International Commercial Contracts. The guidance on the interpretation and application of the choice-of-law rules contained in para. 2 of the Principle generally stemmed from the previous draft clarifying the position in the 'code is law' debate and aiming to avoid producing unclear outcomes or disrupting the functioning of the network relevant for the digital asset.

52. Regarding the rules on applicable law in case of insolvency, these were left substantially the same with further clarification of the usual exceptions that defer to the applicable insolvency laws. The guidance on the interpretation and application of the choice-of-law rules contained in the Principle generally stems from the previous draft clarifying the position in the 'code is law' debate and aiming to avoid producing unclear outcomes or disrupting the functioning of the network relevant for the digital asset.

53. Regarding this Principle, the following Steering Committee comments are especially noteworthy:

Japan:

Principle 5 (2)(c) stipulates “The choice of the applicable law can be included in the code...” Considering that normal participants in transactions of digital assets will not have ability to read the choice in the code, it is questionable if such choice in the code could be considered visible and be an effective choice of law (there seems to be the difference in the level from choice of law in forms prepared by one party).

It is not clear how the Principle 5 (2) is applied to proprietary questions in custody.

Turkey:

Considering the global scale of digital asset transactions, this paper believes that, factual connection of a system of a digital asset should not be based on where the digital asset is issued or its current location as a general rule, as it would be hard for individuals to claim their rights in different jurisdictions. We believe this won't be fair especially for consumers or unqualified investors as this will put capital and time-consuming burden on the individuals to file law lawsuits and follow-up proceedings in various jurisdictions.

As a recommendation, an alternative dispute resolution policy/rules for disputes concerning digital assets could be formed and implemented as in the case of WIPO-initiated Uniform Domain Name Dispute Resolution Policy.

That said, a hybrid system can be embraced by the states. The hybrid system should be two-fold. When disputes arise out of the digital asset and not the linked asset, arbitration or mediation rules should be applied specifically designed for this type of disputes. On the other hand, when the disputes originating from “asset” linked or tethered to the digital asset, (a) if the asset is tangible applicable law should be the law of where the asset is first issued; (b) if the asset is intangible the applicable law should be determined based on the intangible asset's location and (c) if the digital asset is 'linked' to shares or bonds, applicable law should be the law of issuer of these bonds and shares (e.g. the headquarter of the company which its shares have been tokenized)

Alternatively, instead of trying to clarify the determination of the strongest factual connection, this issue may completely be left for the other laws to govern. There are two risks need to be balanced here: If any particular factual connection is to be determined, given that the proprietary rights are governed by the other law, the differences in the other law may cause even bigger problems than the factual link is supposed to resolve. If it is left to the other law to govern the details, this creates space for the legal uncertainty even at the beginning of the transaction. Provided that they the parties have the opportunity to choose a law, the risk may be left on the parties.

Additionally, considering that the transferee may be vulnerable in certain transactions, it could be discussed whether it would be beneficial to have rules in place to protect the transferee (i.e. priority to the transferee's jurisdiction may be given to have that state's rules apply in cases of dispute), such as in the cases of consumer protecting measures to ensure access to justice.

Mexico

My concern regarding questions is that there are two different areas where digital assets can operate: One, in the commercial and personal transactions of individuals and, another, in those digital assets that are included in the scope of the financial laws and financial institutions.

SECTION III: CONTROL

Principle 6: Definition of **control**

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

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

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

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

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

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

(2) A change of control includes the replacement, modification, destruction, cancellation, or elimination of a digital asset and the resulting and corresponding derivative creation of a new digital asset (a "derivative resulting** digital asset") which is subject to the control of another person.**

(3) An ability for **the purposes of paragraph (1)(a) need not be exclusive if and to the extent that:**

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

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

Commentary

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

1. The exclusive ability requirements in paragraph (1)(a) of this Principle (as relaxed in paragraph (3)) recognise that the ability to exclude is an inherent aspect of proprietary rights (i.e., proprietary interests or rights with proprietary effects). These requirements contemplate that 'control' assumes a role that is a functional equivalent to that of 'possession' of movables. [Whether 'control', as defined in this Principle, exists is a matter of fact and does not depend on a legal conclusion. However, as explained below in paragraph 3, the presence of control gives rise to legal consequences.](#) The exclusivity criterion of control (including the standards for its relaxation) appears to reflect the norm in the relevant markets for digital assets. Acquirers expect and believe that they have obtained the relevant exclusive abilities with respect to a digital asset (subject to understood exceptions) and in fact that generally has been the case.

2. Because control assumes a role that is a functional equivalent to that of 'possession', a State may wish to consider using a term other than 'control' (e.g., 'possession') if necessary or helpful to accommodate other aspects of its legal system. However, 'possession' in this context is a purely factual matter and not a legal concept. [Therefore, while being akin to the concept of 'possession' as used in certain jurisdictions, control as used in these Principles must not be understood to be identical to such possession: where in certain jurisdictions possession is a legal concept and a possessor may 'hold' an asset through another person, under these Principles control is a factual matter and a person](#)

[cannot control a Digital Asset through another person unless the criteria of this Principle 6 are met. On the holding and custody of Digital Assets, see also below, Principle 12.](#)

3. The concept of control in a law governing digital assets serves as a necessary (but not a sufficient) criterion for qualifying for protection as an innocent acquirer of a digital asset (other than as a client in a custodial relationship) and as a method of third-party effectiveness (perfection) and a basis of priority of security rights in a digital asset. States also may choose to adopt the concept of control as an element of third-party effectiveness of proprietary interests more generally. [It is important to note that control \(as defined in this Principle\) is also an element in the definition of 'digital asset' in Principle 2\(2\): only an electronic record which is capable of being subject to control is a 'digital asset' and therefore within the scope of the Principles.](#)

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

5. [Control by a person of a digital asset as agent \(for example, an employee may have control for their employer\), then that is treated in these Principles as the control of the principal.](#) The concept of control also ~~may be~~ relevant in the context of the custody of digital assets ~~in an arrangement. As set out in which a custodian is~~ Principle 12, [under a custody agreement a service provider is obliged to hold \(ie, administer\) digital assets for its clients, either by controlling the digital assets itself or by entering into an custody agreement with a sub-custodian whereby the sub-custodian controls the digital assets.](#) The private law (as well as a regulatory framework) may require a custodian to maintain control of digital assets held for clients. This is an example of one person (the custodian) having control while proprietary rights are transferred to or remain with another person (the client). A thief of digital assets would be another example of the separation of control and proprietary rights.

Explanation and commentary

'Ability' of a person with control

6. **1.** — In this Principle the term 'ability' is used instead of the term 'power'. While the terms have identical meanings, 'ability' is more compatible with the concept of control as a factual standard and 'power' has a more 'legal' connotation. On the exclusivity aspect of required abilities, see paragraphs ~~[3-9],~~ [infra 8-12 below](#).

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

Exclusivity of abilities

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

which the keys are stored, or otherwise. This underscores the distinction between a change in control and a transfer of proprietary rights.

~~9.~~ ~~4.~~ — Even if a person were to obtain the relevant abilities without the consent of the rightful control person, the rightful control person would continue to have control until such time as it no longer possessed the requisite abilities (e.g., because control had been transferred to another person). The exclusive abilities contemplated by paragraph (1)(a)(i) and (ii) assume the existence of a system for digital assets that reliably establishes those abilities and their exclusivity. But the abilities and exclusivity are not negated by the possibility that such a reliable system might be compromised by a wrongful “hacking”—even if such a wrongful compromise actually occurs. Such a possibility is an inherent, if unfortunate, attribute of any digital asset. As a practical matter, however, past experience indicates that the occurrence of such a hack would be likely to result in a prompt transfer of control by the wrongdoer. See also Principle 7, Comment 2.

~~9.10.~~ Paragraph (3) provides explicit relaxation of the exclusivity requirements imposed by paragraph (1)(a). Paragraph (3)(a) contemplates situations in which the inherent attributes of a digital asset or the system in which it resides ~~impose~~ may result in changes, including a change in control, which constitute exceptions to the exclusivity of a control person’s abilities. ~~It recognizes that in many cases a person in control will not have abilities that actually are exclusive in a strict, literal sense. Subparagraph (Paragraph (3)(b) recognizes that a person in control may wish to share its abilities with one or more other persons for purposes of convenience, security, or otherwise. For example, in a multi-signature (multi-sig) arrangement, if a person can identify itself under Principle 7 paragraph (1)(b), it could have control even if it shares the relevant abilities with another person. This is so even if the action of the other person is a condition for the exercise of a relevant ability. See Illustration 1, *infra*.~~

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

~~10.11.~~ ~~6.~~ — Paragraph (1)(a)(iii) of this Principle does not require that the specified ability ~~there~~ must be exclusive. Inasmuch as a control person must have the exclusive ability to prevent others from obtaining substantially all of the benefit of a digital asset, it ~~[may] [would]~~ be of no (legal) consequence that a control person has elected to permit another person (or persons) to obtain the ~~benefit~~ benefits (or some of them). It also may be that this situation is already covered by the exceptions provided in paragraph (3)(b), which permits sharing of abilities. If so, whether or not the ability specified in subparagraph (a)(iii) is required to be exclusive ~~[may] [would]~~ be of little or no consequence. In any event, a control person need not prove a negative fact, as provided in Principle ~~7~~ 6 and explained in the commentary thereto.

Illustrations of the application of Principle 6 (definition of ‘control’)

Illustration 1: Shared control and multi-sig arrangements.

~~11.12.~~ Investor acquires proprietary rights in a digital asset (cryptocurrency) held in a public blockchain platform. Investor holds through a multi-sig arrangement in which the two of three private keys—the Investor’s private key and the private keys of X and Y, parties trusted by Investor—are required to change control of the digital asset. Assuming Investor has all of the abilities specified in paragraph (1)(a) of the Principle and can identify itself as provided in paragraph (1)(b), Investor has control over the digital asset. Although Investor has shared the ability to change control specified in paragraph (1)(a)(i) and action by X or Y is a condition for Investor to exercise that ability, paragraph (3)(b) provides an exception to the exclusivity requirement of paragraph (1)(a)(i).

Continued Issued Paper

54. During the 101st Session of the Governing Council (Rome, 8-10 June 2022), two comments were made regarding the definition of control. First, a Member of the Governing Council, raised a query regarding the wording of Principle 6(3), seeking confirmation as to whether it was intended to reflect the factual notion of control. In response, it was confirmed that the wording of the Principle was intended to be consistent with the factual notion of control.

55. Additionally, a representative of UNCITRAL noted that the DAPL Project appeared to depart from other international instruments, including the UNCITRAL Model Law on Electronic Transferable Records, with regard to the use of the legal notion of control rather than the factual one. It was suggested that an effort should be made to make the Principles consistent with other such instruments. In response to this, it was explained that the DAPL Project gave preference to the factual notion of control over the legal one because in some jurisdictions, certain legal concepts might be non-existent. It was emphasised that the Project was generally concerned with basic situations of custody, control, transfer, and secured transactions, and that no matter how a given legal system characterised the rights, the goal should be the same – harmonisation and legal certainty in a global market. Accordingly, at this stage, the Project's notion of control was factual and not legal, which did indeed differ from past instruments such as the Geneva Securities Convention and the UNCITRAL Model Law. It was noted that the commentary should be revised to further elucidate this.

56. At DC8, the Drafting Committee members discussed the feedback regarding the definition of control provided at the Governing Council Session as well as by the Steering Committee's first round of comments. Regarding the comments made during the Governing Council session, the Drafting Committee members were of the view that the concerns raised could be regarded mainly as a matter of interpretation of terms. Drafting Committee members held that the Principle on control, while a factual notion, also contained within it a legal concept as there were other rules contained in the Principles (e.g. the scope of the Principles, the element of perfection, and the right of innocent acquisition) which – when combined with the definition of control – made it such that the definition of control was not only a factual one but also one having a legal effect. The difference was that while the definitions of control used in other instruments turned on certain legal conclusions, the DAPL Principles turned on the factual powers of control. In this they differed in what was required to prove control, however, but it was still a legal construct. Accordingly, it was suggested that the wording could be improved to reflect this nuance, and that this further elucidation might be included in the Commentary.

57. The Drafting Committee further suggested that the definition of control was in line with the notion of control as defined by the UNCITRAL Model Law on Electronic Transferable Records. The Working Group Chair explained that some commentators objected to the definition of control as a functional equivalent of possession over an intangible thing, since possession was a legal notion. Nonetheless, it was noted that since the Principles did not use the concepts of constructive control or constructive possession, DAPL was consistent in its use of the notion of control.

58. The Drafting Committee also examined the question of whether the concept of constructive possession should be included in the commentary and finally decided against doing so. In this respect, the Drafting Committee noted that one of the comments in the Steering Committee feedback raised the idea of constructive possession. Following discussion of where the interaction of control and custody should be discussed, it was agreed that agency and control over custodians should also be elaborated upon. The definitions were to be linked more closely with exclusiveness of the ability to control. The suggestion to introduce the concept of rivalrousness into the scope of the Principles and commentary was rejected, due to the difficulties it would introduce.

Principle 7: Identification of a Person in Control of a Digital Asset
~~Asset~~ digital asset

(1) In any proceeding in which a person’s control of a digital asset is at issue,

(a) it is sufficient for that person to demonstrate that the identification requirement in Principle 6 ~~paragraph (1)(b)~~ is satisfied ~~as to~~ in respect of the abilities specified in Principle 6 ~~paragraph (1)(a)(i) and (ii)~~;

(b) ~~—it is not necessary for~~ if that person ~~to prove~~ demonstrates that ~~no person other than the person in control and those permitted by paragraph (3)~~ it has any of the abilities specified in Principle 6 ~~paragraph (a)~~ (i) and (ii), those abilities are presumed to be exclusive.

(2) The identification mentioned in Principle 6 ~~paragraph (1)(b)~~ may be by a reasonable means including (but not limited to) an identifying number, a cryptographic key, an office, or an account number, even if the identification does not indicate the name or identity of the person to be identified.

Commentary

1. Only in a litigation context (broadly construed) would an issue arise as to which person has control of a digital asset under a digital assets law that includes the criteria specified by this Principle. If the control of a person is challenged, it would be impossible for the putative control person to prove with certainty a negative—that no person other than one permitted by the definition has the relevant abilities. Paragraph (41) of the is Principle makes it clear (although it would be implicit in any event) that a person asserting that it is in control of a digital asset meets its burdens of production and persuasion by showing that it has the specified abilities. It need not prove the negative—that no one else has the abilities—in order to prove that it has control. The first alternative subparagraph (b) makes this clear. The second alternative subparagraph (b) would dictate the same result through the operation of a presumption, the operation of which would be governed by the applicable domestic procedural law. Of course, a person who was previously (rightfully) in control may demonstrate under applicable domestic law that it has a better proprietary interest than the person currently in control by proving that the change of control was wrongful.

2. As a practical matter, there is little chance that another person would appear in a contested proceeding to claim that it has the relevant exclusive abilities without the putative control person’s consent. Under the criteria, that other person also would not have control. Any concern about such a person (e.g., hacker, thief, or finder) appearing to make such a claim seems unwarranted. Moreover, experience has shown that in situations in which the relevant abilities have been obtained wrongfully the abilities have quickly been exercised and the assets have been removed from the control of the original control person. This reflects a set of risks that are inherent in digital assets.

Continued Issues Paper

59. All changes to Principle 7(1)(a) and Principle 7(2) relate to amendments made for cross referencing and clarity.

60. For Principle 7(1)(b), which relates to the relevance of exclusivity of control in identifying a person in control of a digital asset, two options were considered. Option 1 related to there not being a need to prove exclusivity, whereas option two assumed exclusivity of control if the provisions of Principle 5(a)(I) and (ii) are satisfied. The second alternative was proposed at DC7. As noted in the Commentary which explains the two alternatives, the first alternative subparagraph (b) makes it clear that a person asserting that they are in control of a digital asset meets its burdens of production and persuasion by showing that it has the specified abilities, without needing to prove the negative. The second alternative subparagraph (b) would dictate the same result through the operation of a presumption. At DC9, the second option was retained in the draft.

61. On this Principle, a representative of the Netherlands from the Steering Committee has noted:

Possibly 7(1)(b) could be rephrased as a rebuttable presumption: the person who demonstrates what is said in 7(1)(a) is presumed to have control unless another party provides stronger evidence to the contrary. In other words, use the procedural notion of presumption instead of formulating it as a definite identification.

I also wonder whether it should not be mentioned that a person should be able to explain how he came to be in control, as in certain cases the history shows that the asset was at one point 'stolen'. Dutch law principles would point against allowing a stolen object to be obtained by good faith if it is clear that the object was stolen (of course, it is debatable whether the asset history needs to be consulted or not). (this is partly covered by principle 9 on the innocent acquirer, but that aspect should also be part of the question of establishing control).

62. This comment has been reflected in the updated draft.

SECTION IV: TRANSFER

Principle 8: Acquisition and ~~D~~isposition of ~~D~~igital ~~Assets~~digital assets

~~(1)~~—~~(a)~~ The transfer of a digital asset is the change of a proprietary right from one person to another person.

~~(b)~~—2 A transfer of a digital asset includes the replacement, modification, destruction, cancellation, or elimination of a digital asset and the resulting and corresponding derivative creation and acquisition of a ~~derivative~~resulting digital asset.

Commentary

1. Paragraph (1) addresses not only the transfer of a digital asset from one person to another person but a transfer that results in the acquisition of a derivative digital asset that is not the same digital asset that was disposed of by the transferor. An example of such a derivative digital asset is the UTXO (unspent transaction output) generated by a transaction in Bitcoin. Another example might be adjustments in balances in accounts resulting from transactions in ether on the Ethereum platform, as to which the digital asset that is disposed of and the digital asset that is acquired are fungible assets and not necessarily the “same” asset.¹²

2. The word ‘transfer’ in these Principles includes the grant of a security right in favour of a secured creditor, and the word ‘transferee’ includes a secured creditor.

¹² This comment is similar to Principle ~~6~~5, Explanation and commentary, paragraph 2. Ultimately the point of these comments might be made as a part of only one of the Principles with that Principle containing only a cross-reference to other relevant Principles.

Continued Issues Paper

63. At WG5, as indicated in the report at Paragraph 106, the WG requested the DC to come up with a better term for 'derivative' digital asset, given the legal implications of the use of this term. As such, at DC7, it was agreed that the use of the word 'resulting' digital asset was better suited in describing the types of transactions which this Principle was referencing.

64. With regard to this Principle, a representative of the US in the Steering Committee noted several points including:

"We are concerned about the use of the term "right." That term may imply a legal right that may not exist. For example, if a hacker transfers a digital asset to an innocent purchaser, the innocent purchaser acquires the digital asset free of competing property claims even though the hacker, being a thief, had no legal right to the digital asset let alone the legal right to transfer it. Perhaps "power" would be a better term instead of "right."

65. In this regard, the DC is considering various points which such a revised commentary could cover:

- a. It could refer back to Principle 6 Commentary paragraphs 4 and 5, and explain that a transfer of proprietary rights is a different concept from a change of control.
- b. To dovetail that Commentary to Principle 6 with the commentary to Principle 8.
- c. In some situations (and under some laws), a change of control does not transfer proprietary rights because it is not intended to do so. One example of this could be the change of control from the owner of a digital asset to a custodian. Another could be theft of a digital asset. In other situations, there is an intention to transfer proprietary rights, but the transferor has no proprietary rights to transfer (e.g. when the thief sells the digital asset to someone else). It is in the latter situation that the innocent acquisition rule applies.
- d. The Commentary would need to make it clear, therefore, that for the purposes of the Principles, 'transfer' is defined in order to give meaning to (i) the word 'transferee' in Principles 9 – 11, and (ii) the grant of security rights in Section VI. The Commentary would therefore have to say that a 'transfer' means the situation in which the transferor intends to transfer a proprietary right to the transferee and either has the right to do so or the power under Principle 9.
- e. Presumably 'transfer' is also wider than change of control, since a proprietary right could be transferred in a digital asset without a change of control. An example would be an off-chain transfer. In this regard, representatives of Turkey, Italy, and Iran have made the following comments with examples respectively:

Turkey:

In terms of blockchain, on-chain transactions mean cryptocurrency transactions that take place on the blockchain and in order to ensure validity remain dependent on the state of the blockchain. For example, transfer of bitcoin or Signum (formerly known as Burstcoin) from a lender to a debtor.

Transactions conducted outside the blockchain platform is considered as "off-chain transfer". A third party can verify such transaction. For instance, exchange of private keys. Again, transferring a digital asset via transferring a usb driver (cold wallet) itself could be an example for an off-chain transaction.

Another way of transferring control over certain digital assets would be to reveal the account credentials (where the digital assets are stored/access thereto is made

available) to another person so that she/he can have access to the digital assets in that account.

Examples for transfers involving Layer-1 digital assets could be the burning of Ethereum, Solana, Cardano or Avalanche and creating another one for an acquirer.

On the other hand, examples for transfers involving Layer-2 digital assets could be, usage of MATIC for settling and paying for transactions between users in the Polygon network or usage of LRC token for powering the of Loopring platform's operations.

Italy:

1) on chain: any transfer of assets performed on a specific blockchain, such as BTCs' transfer on Bitcoin blockchain

2) off chain: any transaction occurring on a network moving values outside the blockchain. Different methods can be used: the exchange of private keys representing a fixed amount of tokens on the basis of an agreement between private parties; the transaction between private parties agreeing on a debt between them, with the chance for multiple mutually trusting parties to participate, creating a network of value owed from one to the other (e.g., RippleNet, a payment network, allows these operations, using an automated ledger to record all the mutual debts between participating parties); a transfer agreement guaranteed by a third party (e.g., present day payment processors works this way, such as PayPal).

3) layer-1: every transaction performed on a base blockchain such as Bitcoin or Ethereum (main networks within their digital ecosystem)

4) layer-2: a) Ethereum developed a layer-2 solution called Polygon, a decentralized scaling platform providing instant transactions. Many popular DeFi and NFT applications, including SushiSwap, OpenSea, Curve Finance, have integrated with this layer 2 solution; b) Lightning Network is a layer-2 solution developed by Bitcoin which allows individuals to transact not only using BTC but also using different currencies which integrated this solution, such as Litecoin.

Iran:

1. Neo was founded 2014 and has grown into a first-class smart contract platform. It is backed by a global developer community who continue to drive the blockchain forward. It is A cryptocurrency with a relatively fast transaction speed (<https://neo.org/>);

2. Burstcoin (BURST) is another coin that not only has faster block time than mainstays like Bitcoin, it also uses far less energy to mine coins because of its proof of capacity system (<https://www.burstcoin.ist/>).

Off-Chain transfer of digital assets

1. Lightning Network is the most promising by far method of building a off-chain transaction system. It is a proposed implementation of Hashed Timelock Contracts (HTLCs) with bi- directional payment channels which allows payments to be securely routed across multiple peer-to-peer payment channels. This allows the formation of a network where any peer on the network can pay any other peer even if they don't directly have a channel open between each other. Very little third-party trust is required.

2. Credit-Based Solutions. The simplest example of an off-chain transaction is perhaps two friends who agree on a debt between them. The "transaction" happens by the act of agreeing that the debt exists, and the validity of it is based solely on the trust that one friend has in the other. Further transactions can be agreed upon,

possibly in exchange for something of value such one friend buying the other a meal. Multiple mutually trusting parties can participate, creating a network of value owed from one to the other. As an example the Ripple monetary system takes this concept, and adds to it an automated ledger to record all the mutual debts between participating parties. However actually acting upon those debts is still a matter of trust between the parties; the system only records debts and can-not by itself causes Bitcoins or some other object of value to change hands. In theory, the use of multi-signature techniques offers the promise of secure Off-Chain transactions. However, the practical applications of such "CryptoCubic" approaches have yet to be confirmed.

3. Trusted Third Parties. If the sender and recipient do not trust each other, or would simply prefer someone else record and guarantee the transaction, they can use a trusted third party to record and guarantee the transaction. The vast majority of conventional banking and electronic payment systems work this way. For instance in the PayPal system.

- f. The Working Group may consider paying additional attention to this issue, keeping in mind that it might be very technologically specific.
- g. The commentary should explain the distinction between a transfer off-chain where there is no change of control, and therefore Principle 9 does not apply (9(1))(c)) and an on-chain transfer where there is a change of control and Principle 9 does apply.
- h. Should the Commentary say anything about transfer more generally, even if it is just to say that, apart from the application of the innocent acquisition rule in Principles 9 – 11, whether any particular situation results in a transfer (of proprietary rights) is a matter for 'other law'?

66. Paragraph 2 of the Commentary for this Principle was the result a request from WG5 asking for further clarity on the meaning of 'transfer' and 'transferee' in these Principles, in the context of secured creditors.

Principle 9: Innocent Acquirer Rule

~~(1) — The law should include an innocent acquirer acquisition rule, specifying~~

~~(a) — the requirements for a transferee to qualify as an innocent acquirer of a digital asset or (1) (a derivative digital asset and~~

~~(b) — the rights obtained by an innocent acquirer of such an asset.~~

~~(2) — In this principle, the term 'digital asset' includes a derivative digital asset.~~

~~(3) — The requirements and rights referred to in paragraph (1) should be equivalent to those found in good faith purchase, finality, and take-free rules).~~

~~(4) — The innocent acquirer rule should provide that~~

~~(a) — an) An innocent acquirer takes a digital asset free of conflicting proprietary rights ("('proprietary claims'").~~

~~(b) — no No rights based on a proprietary claim relating to a digital asset [may][can] be successfully asserted against an innocent acquirer of that digital asset.~~

~~(c) — Control In order to qualify as an innocent acquirer, a transferee must obtain control of a digital asset should be an essential element for qualifying as an innocent acquirer, and.~~

~~(d) — An innocent acquirer [may][can] acquire a proprietary right in a digital asset even if control of that digital asset is changed by a person that who is acting wrongfully and has no proprietary right in the digital asset.~~

(2) In this Principle, the term 'digital asset' includes a resulting digital asset.

(3) The requirements in a State for a transferee to be an innocent acquirer should be equivalent to those found in relevant good faith purchase, [finality,] and take-free rules of that State.

Commentary

1. The rights conferred on IA innocent acquirers in accordance with subparagraphs (a) and (b) of paragraph (41) mean that digital assets will have attributes similar to those of negotiability under rules applicable in some jurisdictions to negotiable instruments, negotiable documents of title, and negotiable certificated securities.

2. Subparagraph (d) of paragraph (41) is intended to make clear that, for example, even if an acquirer receives control of a digital asset by a change in control made by a thief or a hacker, the acquirer may qualify as an IA innocent acquirer. See also the discussion in Principle 6, Explanation and commentary, paragraphs 3 and 4.

~~(5) — In specifying who falls within the definition of an innocent acquirer, consideration should be given to (but not limited to) the following:~~

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

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

~~(c) in relation to knowledge, an acquirer's actual knowledge;~~

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

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

~~(f) an acquirer's acquisition for value given by the~~³. As indicated by paragraph (3) of this Principle, a State has flexibility as to the precise contours of the requirements for innocent acquisition of digital assets that it adopts, given that such requirements need to be consistent with the good faith purchase and take free rules of that State. A State might wish to adopt slightly different innocent acquisition rules for different types of digital assets.

(4) If these Principles are applied pursuant to Principle 5(1)(c)(i), the following requirements for a transferee to be an innocent acquirer apply unless the law of the forum State provides otherwise, consistent with paragraphs (1) to (3) of this Principle, with respect to digital assets of the relevant type:

(a) A transferee of a digital asset is an innocent acquirer or received by of a digital asset unless, at the transferor;

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

~~(h) transferee takes control of the test adopted in digital asset, the Geneva Securities Convention, Article 18(1), i.e., whether:~~

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

~~(6) If~~ (b) In determining whether a person ought to know of an interest or fact:

(i) the determination must take into account the characteristics and requirements of the relevant market for the digital asset; and

(ii) the person is under no general duty of inquiry or investigation;

(c) An organisation actually knows or ought to know of an interest or fact from the time when the interest or fact is or ought reasonably to have been brought to the attention of the individual responsible for the matter to which the interest or fact is relevant.

(d) A transferee of a digital asset is not an innocent acquirer rule if the transfer of the digital asset is made by way of gift or otherwise gratuitously [and is not the grant of a security interest].

(5) If a transferee is not protected by paragraph (1), other law determines the rights and liabilities, if any, of that transferee.

4. Paragraph (4) provides ~~that qualification as~~ a default set of requirements for a transferee to be an innocent acquirer ~~requires the absence of notice or knowledge, the law should specify the effect of a transferee's notice or knowledge, including~~ for use if (a) a State's court needs, in the course of litigation, to apply the Principles pursuant to the choice of law rule in Principle 5(1)(c) and (b) that State has not yet adopted its ~~impact on the claims~~ own innocent acquisition rule for digital assets of the relevant type. If the State has adopted its own rule, that rule would apply as Principles law. Paragraph (4) is drawn substantially from the innocent acquisition rule in the Geneva Securities Convention.

5. Paragraph (5) reflects Principle 3(3), which states that, except as ~~to which a transferee does and does not take free~~ displaced by these Principles, other law continues to govern issues relating to a digital asset.

Continued Issues Paper

67. Several parts of this Principle have been reordered and some have been merged with each other. This is so that the Principle takes a more affirmative approach. Several parts are now also consistent with the Geneva Securities Convention. Additionally, following the input of representatives from the Steering Committee on the complexity of the original draft, some redrafting was done by the Drafting Committee to make this Principle easier to understand.

68. More specificity has been included in order to ensure that the Principle works well in the context of Digital Assets.

69. Principle 9(3) offers guidance to States on how a good faith purchase rule in a particular jurisdiction can be applied to innocent acquirer's of digital assets.

70. The commentary was expanded to explain that although the nemo dat principle means that not every change in control is equivalent to the transfer of title, for example in scenarios involving a hacker; at the same time, the innocent acquisition rule was introduced to allow an innocent acquirer to obtain the title to the digital assets without any competing claims thereto.

71. A comment from a representative of the Netherlands from the Steering Committee was also considered:

I also wonder whether it should not be mentioned that a person should be able to explain how he came to be in control, as in certain cases the history shows that the asset was at one point 'stolen'. Dutch law principles would point against allowing a stolen object to be obtained by good faith if it is clear that the object was stolen (of course, it is debatable whether the asset history needs to be consulted or not). (this is partly covered by principle 9 on the innocent acquirer, but that aspect should also be part of the question of establishing control).

72. It is noted that the Working Group did not prefer this approach at WG5. However, this issue may be reconsidered.

73. A representative of Turkey from the Steering Committee raised the following point:

For instance, in case of purchasing an NFT which is minted by infringing a trademark right, the acquisition could be deemed valid if the third party purchasing this NFT is in good faith. However, if the NFT acquirer could/is expected to know that the acquisition is wrongful as to the holder of the proprietary claim, for instance when a very famous designer's bag or well-known scenes of a movie is minted as an NFT [Since the Principle 9(5)(b), (d) or (e) might be applicable], the acquirer should not enjoy the innocent acquirer principle. (Still, in some cases it may not be reasonable to expect the acquirer to know of the legal relationship between the IP right holder and the infringer. For instance there could be a license agreement between the parties, or it may not be possible to know the issuer of the NFT. As such, this provision should be carefully drafted.)

74. A representative of Japan from the Steering Committee raised the following point on this Principle:

When a digital asset that is linked to another asset is innocently acquired, what happens in the another asset? If there is a legal link under the applicable law, is the innocent acquirer automatically innocently acquire the another asset? Principle 16 (4) suggests that innocent acquisition of the digital asset is covered by the Principle, but how such innocent acquisition of the digital asset affect the acquisition of the another asset is the matter covered by other law than the digital asset law. However, in case of negotiable instruments, we do not discuss innocent acquisition of "paper" independently of innocent acquisition of "claims."

75. On this, it is noted that other law would determine whether the other asset is also acquired free of conflicting claims, e.g. if a digital asset was treated as a negotiable instrument then the linked asset would also be acquired free of claims. This will be made clear in the Commentary. It is noted that the DC will insert additional examples and Commentary on this Principle ahead of the next meeting of the WG. This include incorporating input received from the Steering Committee regarding the participants of a blockchain and how they are very often anonymous.

Principle 10: Shelter ~~principle~~rule

~~{The law should provide that} [A][a]~~An initial transferee from an innocent acquirer and any subsequent transferee ~~should have~~has the same protection as the innocent acquirer from conflicting proprietary rights and the successful assertion of proprietary claims.

Continued Issues Paper

77. The Chair of the DC had requested input at WG5 on whether 'The law should provide that' should be included at the beginning of each Principle. This was generally not seen as necessary. As such, this has been deleted. Additionally, 'should have' has been replaced with 'has' to add additional clarity to this Principle.

78. It is noted that the DC will insert additional examples and commentary on this Principle ahead of the next meeting of the WG.

**Principle 11: Application of ~~Innocent Acquirer Rules~~innocent acquisition rule
to a ~~Custody Relationship~~custody relationship**

~~{The law should provide that}~~ A client ~~that~~who acquires a proprietary right in a digital asset ~~through a custody relationship with~~that is held for that client by a custodian

- (a) takes its right free of conflicting proprietary claims, or
- (b) that no rights may be asserted against the client based on a conflicting proprietary claim, or
- (c) both (a) and (b),

subject to substantially the same conditions that apply under the innocent ~~acquirer~~acquisition rule in Principle 9 (but without a requirement that the client obtain control over the digital asset).

~~Commentary~~

Commentary

1. This Principle is intended to confer on a Client in a custodial relationship substantially the same benefits conferred on an ~~IA~~innocent acquirer under the ~~IAR~~Innocent Acquisition Rule in Principle 9. However, the doctrinal approach may be different in the case of a Client in a custodial relationship. For example, the Client's proprietary right may be in a fungible bulk of digital assets. Moreover, in a custodial relationship it would be the Custodian that would be in control of the relevant digital asset(s) and not the Client. This Principle should be coordinated with Section IV. [Note: Consideration should be given to a variety of contexts in which questions as to the nature and extent of propriety rights may arise in the context of custodial relationships.]

Continued Issues Paper

79. Principle 11 undergone stylistic and drafting corrections to improve the consistency of the present Principles.

80. On this, a representative of the United States from the Steering Committee queried:

It is unclear how the custodian relationship works in the following context. The custodian acquires a digital asset subject to a competing property right and credits the digital asset to the client's account at the custodian. The client has no notice or knowledge of the competing property claim. Does the client acquire the digital asset from the custodian free of or subject to the competing property claim?

81. The Principles suggest that such a client would take the asset free of the competing claims. It is noted that the DC will insert additional examples and commentary on this Principle ahead of the next meeting of the WG, including those which address issues raised by the Steering Committee.

82. Additionally, a representative of Luxembourg from the Steering Committee has commented:

Two examples come to mind: (i) If the custody relationship is to a pool of assets, so each single asset is not allocated to an individual owner/customer, then what rule applies to the priority between the owners/customers when the custodian is insolvent and there are not enough assets in the pool for all the owners/customers?

(ii) If, on the contrary, it is specified in the custody relationship which individual assets that belong to each owner/customer, who prevails if the custodian passes the owner's/customer's assets on to an innocent acquirer (third party)?

Please bear in mind that the innocent acquirer rule will de facto, lead to liability of the custodian as the moment the custodian accepts the assets in custody someone else will loose the asset. In turn, the custodian rules must provide that this liability function is fully understood; where we have a similar function in banking law, usually the true risk that the innocent acquirer rule has any effect is Zero, since all custody chains are built up hierarchically. The situation is different with regard to decentralized stored crypto-assets. I hence caution that the Principle, if we want to avoid systemic risk, may prompt the need of some thorough rethinking of the applicable custodian rules (minimum capitalization, due diligence etc.). These are, however, in the remit of financial regulation. I thus emphasize my previous argument to abstain from "financial regulation through the backdoor."

83. The DC will prepare additional Commentary to address these issues, including the matter of the application of this Principle to off-chain transactions. Additionally, the Principle will be redrafted for reasons of style, as well as the discussion of its content at WG6.

84. Furthermore, the WG may give consideration to moving this Principle into the section on Custody.

SECTION V: CUSTODY

Principle 12: Custody

(1) This Principle applies when, in the course of a business and pursuant to an agreement, (a "custody agreement"), a person (a "custodian") holds a digital asset on behalf of a client in a manner that the digital asset so held is not available to the creditors of the custodian if the custodian enters into any insolvency proceeding, [and that the custodian owes duties to the client]. ~~The agreement between the custodian and the client is a "custody agreement."~~

Commentary

~~Commentary~~

1. This Principle applies to custody, that is, to situations where a person (usually a legal person, often a regulated entity), ~~holds~~controls a digital asset on behalf of and for the benefit of another, typically a client, though it could be another custodian, in a manner that gives the client (or other custodian) special protection against unauthorised dispositions of the asset and against the insolvency of the custodian ~~who controls the digital asset~~. It only applies when the person providing the custody services does so in the course of a business. The special protection for the client referred to is likely to be achieved in private law by the client having a proprietary right of some sort in the asset. The precise analysis by which this protection is achieved will vary according to the private law of the relevant jurisdiction. As mentioned in paragraph 5 of the commentary to Principle 6, custody is an example of a situation where one person controls a digital asset while another person (the client) typically has a proprietary right in that asset.

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

3. The purpose of this Principle is to set out principles relevant to custody of digital assets. This first paragraph is a general statement explaining the core situation in which there is a custody agreement and in which a person acting in the course of a business is a custodian. It is designed to be helpful to the reader and is not drafted as a legal definition. There will be situations when there is a custody agreement where the custodian does not hold a digital asset on behalf of a client: (1) if the client has not yet transferred a digital asset to the custodian or the custodian has not yet received it on behalf of the client; (2) when the custodian has exercised a (limited) right of use (see Principle ~~13~~12(1)); or (3) if a custodian breaches its obligations and fails to hold the digital asset that is the subject of the custody agreement. Moreover, it is difficult to see how a person (in the course of a business) could hold an asset on behalf of a client in a way that it is available to the 'custodian's' creditors generally since if this is the case the 'custodian' would have complete ability to use the asset as its own and the asset would not be held on behalf of the client. The general statement, however, captures the two critical points of custody, namely, that in most situations the 'custodian' holds the asset (and the client does not) and yet the asset does not form part of the custodian's insolvency estate. 'Hold' is defined in paragraph (2). The commentary at the end of this ~~p~~P Principle explains the different ways in which a digital asset can be held.

(2) ~~In this Section~~

(a) where a digital asset is [considered] fungible, a reference to “a digital asset” or “the digital asset” includes a reference to a certain quantity of digital assets of an identical type to that digital asset;

~~f~~**(b) a custodian holds a digital asset if**

(i) that custodian controls the digital asset, or

(ii) another custodian provides custody services to that custodian in relation to the digital asset.~~f~~

~~Commentary~~**Commentary**

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

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

(3) An agreement for services to a client in relation to a digital asset is a custody agreement if

(a) the service is provided in the course of the service provider’s business;

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

(c) the client does not have the exclusive ability to change the control of the digital asset; within the meaning of Principle 6(1)(a)(i);

unless it is clear from the wording of the agreement that the client does not have the protection described set out in Principle ~~14(3)~~ below: 15(1).

Commentary

~~5-6.~~ Paragraph (3) provides a method to identify whether an agreement is a custody agreement or not. It does two things. First, (a), (b) and (c) serve as a definition of a custody agreement, and therefore of custody. Second, it addresses the line between a custody agreement and an agreement under which any assets held by the service provider form part of that service provider’s assets for distribution to its creditors on its insolvency. This latter type of agreement can look similar to a custody agreement, in situations where the client does not have control of the digital asset, and the service provider maintains an account in which the client’s entitlement is recorded (which is also (or should be) the case under a custody agreement). However, if under such an agreement any assets controlled by the account provider form part of its assets for distribution to its creditors, the client is

exposed to the insolvency risk of the account provider. A client taking on such a risk should be aware that it is doing so, whereas this is not the case under a custody agreement. For this reason, an agreement under which the client does not have control is presumed to be a custody agreement unless it is made clear in the agreement that assets held by the service provider form part of that party's assets available for distribution to its creditors. Paragraph (3) is designed act as an incentive to service providers to make the nature of the agreement clear on its face.

~~6.7.~~ A state may wish to protect a client who enters into an agreement which exposes the client to the insolvency risk of the service provider by regulation. Various options for such regulatory protection are set out in [\[\]-paragraph 18 of the commentary to Principle 15.](#)

[8.](#) The exclusive ability referred to in Paragraph 3(c) is that referred to in Principle 6(1)(a)(i) and therefore is subject to the relaxation of the concept of 'exclusivity' set out in Principle 6(3).

Continued Issues Paper

85. The last sentence of Principle 12(1) has been deleted and incorporated in parenthesis in the second line. This adds additional clarity.

86. Consistent with the request at WG5 to add some additional clarity, particularly on the issue of Sub-Custody, some additional sentences have been added to the Commentary for Principle 12(2).

87. There continues to be bracketed text in the first part of the Principle. This relates to whether or not a point on a custodian owing certain types of duties to a client should be included in the principle itself, or explained in the Commentary. A representative of Mexico from the Steering Committee has suggested removing this bracketed text ('and that the custodian owes duties to the client').

88. A new sentence in the Commentary now explains that duties owed by custodians to clients will generally be detailed in the private law regime of any jurisdiction, and dependent upon the type(s) of right which the client holds against a custodian.

89. The words 'in this section' were removed in order to not make the Principle too narrow. Additionally, with regard to Principle 12(2), (a) will eventually need to be moved earlier in the Principles as it is not just about custody, but (b) will remain as principle 12(2).

90. In part (2) of this Principle, the word 'considered' is in square brackets ahead of the word 'fungible'. The Principles do not define fungibility, and as such, the WG might consider including the bracketed wording in the principle. In this regard, there is a comment from a representative of Luxembourg as part of the Steering Committee:

I am not sure whether the concept of "Fungibility" requires substitutability, as laid out under Principle 12 (2). It is the very idea of decentralized ledgers that all asset flows can be tracked and followed, and hence all individual cryptoassets identified in those transactions. An asset may well be fungible, yet not substitutable. (I am aware that the term 'Non-fungible token – NFT' is in this sense a misnomer).

91. With regard to the change made to Principle 12(3)(c), this is to address the input received at WG5 that exclusivity in this Principle should correspond with exclusivity as explained in Principle 6 relating to Control.

92. At this stage, it is noted that the use of the term 'hold' in the Commentary in the Principles will be rechecked, noting that there are many instances where 'hold' is used colloquially to describe where an investor 'holds' (i.e. owns) digital assets.

93. There are a few comments by the Steering Committee with regard to this Principle for the WG's consideration:

Japan:

Principle 12 (1) stipulates that the Principle applies when a custodian hold a digital asset "in a manner that the digital asset so held is not available to the creditors of the custodian if the custodian enters into any insolvency proceeding...."

However, whether or not the digital asset held by the custodian is available to its creditor is a legal question affected by some elements. It seems strange that the applicability of the Principles depends on such legal question.

The Netherlands:

In principle 12(3)(b) it seems odd to have in a single breath an obligation to obtain and to hold the asset. In Dutch law those are two separate obligations that typically would also fall under different contracts. Obtaining an asset is commission or a related contract, and holding

the asset (unless it is only temporary as part of execution of the commission) would be custody. I would advise to remove the obligation to obtain the asset from this definition. That would also involve the law of financial services which is an extremely complicated area (as the drafters are well aware of).

Furthermore, I wonder whether a tax law expert has been consulted. The precise wording of the legal relationship in holding assets may have consequences for tax law.

94. It is noted that Paragraph 1 of the Commentary points out that a legal conclusion is usually achieved by the client having a proprietary right, but that the analysis will vary between jurisdictions. Additional Commentary has also been added to make this clearer. Additional Commentary could be included on the presumption in Principle 3(3), which is designed to incentivise parties to make it clear to clients whether the legal conclusion applies (by private law means without trespassing into regulation).

95. An alternative option is to not use 'legal culture neutral' terminology and say 'in a manner so that the client has a proprietary right in the digital asset'. However, this might not be preferable as there has been concern about legal culture neutrality and under some circumstances (where the innocent acquisition rule did not apply and the client obtained the digital asset from an unauthorised non-owner) the client would not have a proprietary right, even though the asset would not be available to the creditor of the custodian either.

96. It is noted that other sections use the proprietary right concept, and if defined properly, it could also be considered in this Principle. Importantly, this is not supported by several members of the Drafting Committee as whether any person has a proprietary right in an asset is a matter of 'other law' (Principle 3), and the DC did not want to include a statement that a client had a proprietary right in the Principle itself. This is explained in the Commentary.

Principle 13: Duties owed by a Custodian to its Client**(1) A custodian owes the following duties to its client:**

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

(b) the custodian is obliged to comply with any instructions given by the client to [dispose of] [transfer] the digital asset; and

(c) the custodian owes duties to the client in relation to the safe-keeping of the digital asset or of a pool of such digital assets.

Commentary

1. The language of Principle 13(1) 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.

2. Principle 13(1) sets out duties which are owed by a person providing custody services under an agreement with a client. These are basic duties and a State should not permit them to be excluded by the terms of the intermediary agreement.

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

4. The duty in sub-paragraph (b) makes the basic point that a custodian is a person who must deal with the assets according to the client's instructions. However, this obligation is qualified by any prohibition on such dealing to be found in criminal or regulatory law, any agreement made between the custodian and any third party to which the client has consented or any security right that the custodian may have in the digital asset (see Principle 13(2)).

5. Sub-paragraph (c) merely states that a custodian owes some duties in relation to safekeeping. A state can choose which safekeeping duties cannot be excluded. Some suggestions are contained in Principle 13(3).

(2) Unless prohibited by a provision in the custody agreement [or by law], a custodian may hold fungible digital assets of two or more of its clients in an undivided pool.

6. Principle 13(2) addresses the common situation where a service provider, such as an exchange, holds an undivided pool of assets on behalf of its clients. In a pooled account, the custodian controls a number of fungible digital assets but no assets or private keys are specifically identified on chain as relating to a particular client ~~(see Principle 13(3))~~. Instead, the number of assets the custodian holds for each client is recorded in the books of the custodian. There could be many reasons for this situation, but one possibility is that an exchange executes transfers of digital assets between its clients by book entry rather than by changing the control of the digital assets.

(3) The duties owed by a custodian to its client may include:

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

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

(c) the duty to acquire digital assets promptly if this is necessary to satisfy the duty under [sub-paragraph \(b\)](#);

(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 arising from a digital asset to the client for whom it holds that asset.

[\(4\) Where authorised by a client or by law, a custodian may hold a digital asset for that client through another custodian \(a "sub-custodian"\) if the sub-custodian is bound by the duties set out in this Principle.](#)

Commentary

[7.](#) Principle 13(3) sets out private law duties which a State may wish to ensure are owed by a custodian to its client, although it is for a State to choose whether it wishes to do so. Separately, a State may wish to impose these duties on custodians as a matter of regulation, that is, by imposing duties for which there is no private law redress but breach of which may incur sanctions imposed by the State.

[8.](#) The duty in sub-paragraph (a) is that 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. The duty in sub-paragraph (b) is that the custodian owes a duty to hold assets correlating to those records. Thus, if the record shows that a custodian holds 1 BTC for A, the custodian must control at least 1 BTC.

[9.](#) The duty in sub-paragraph (c) 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.

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

[11.](#) The duty in sub-paragraph (e) 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.

[12.](#) Principle 13(4) makes it clear that a sub-custody structure can be used. Sub-custody is explained in paragraph 5 of the commentary to Principle 12.

Continued Issues Paper

97. In this Principle, the Working Group is invited to further discuss the use of the phrase 'except to the extent permitted by the client and the law'.

98. There are several comments from representatives on the Steering Committee regarding this Principle which the Working Group might consider:

Japan

Principle 13 stipulates the duties of custodians, but it seems unnecessary to have this Principle 13. Though other parts of the Principles relate to proprietary issues, Principle 13 mainly relate to contractual duty of custodians. In addition, such duties of custodian should be the matter covered by regulatory laws of the relevant countries.

Argentina

"The obligations imposed on the custodian towards its client are reasonable and it is appropriate for the Principle to hold that the State should not allow such basic duties to be excluded. The use of neutral and functional language allows the principle to operate in legal systems that establish or qualify such legal relationships in different ways.

Regarding paragraph 13.2, it is logical. However, the issue of transfers of digital assets between clients by means of book entry instead of changing the control of digital assets will have to be analyzed on a case-by-case basis when establishing the law of each country."

99. Additionally, a query was raised from a representative of Iran from the Steering Committee that where a client's account is frozen, the client can no longer have control. As such, consideration could be given to including 'except to the extent prohibited by law' in Principle 13(b).

Principle 14: Other ~~A~~aspects of ~~E~~custodianship

(1) The relationship between the custodian and the client may exist notwithstanding that a third person has [a right or interest in the digital asset](#) or has any right against the client in relation to the digital asset.

Commentary

1. Principle 14(1) makes it clear that the client could (in the relevant jurisdiction) hold the asset on trust for someone else (e.g. the client could be an investment fund or an individual holding the asset for family member) or that the functional equivalent could occur in other jurisdictions.

(2) A digital asset held by a custodian for a client [may be subject to a security right](#)

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

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

Commentary

2. Principle 14(2) permits a custodian to have a security ~~interest~~right in the asset it controls for a client. The client may owe the custodian fees, for which the custodian wishes to be secured, or the custodian may have lent the client money to acquire the assets.¹³ [A security right under paragraph 2\(a\) could be perfected by control under Principle 17\(1\).](#)

¹³ ~~———— Taking security over digital assets is addressed in the Secured Transactions Principles prepared by SG3 where the secured creditor's interest is called a 'security right'. SG3 probably says something about the security right being automatically perfected in this situation (that is the US position) although this is inconsistent with the Financial Collateral Directive in the EU and the relevant regulations in the UK as currently interpreted.~~

Continued Issues Paper

99. The additional language inserted into Principle 14 was approved at DC 8 and was added to provide additional clarity to the reader, insofar as third-party rights or interests over a digital asset, as opposed to a right or interest against the client in relation to a digital asset.

100. The additional line added to the Commentary of Principle 14(2)(b) is for the purposes of providing additional clarity to the reader. This was inserted at DC7.

Principle 15: Insolvency of custodian

(1) If a custodian enters into any insolvency proceeding, a digital asset that it holds for the account of a client does not form part of that custodian's assets for distribution to its creditors.

Commentary

~~12. Principle 14(3) sets out the consequences of the insolvency of the custodian in a functional way rather than using legal concepts such as property or ownership. On the custodian's insolvency, assets it controls for clients as custodian are not part of the distributed estate. If a holder is not a custodian, any assets it controls will be part of its assets for distribution to its creditors. The effect of C.3 is that any agreement which has the three characteristics of a custody agreement set out in C.3 will attract the consequences in C.9 unless the agreement makes it clear that this is not the case.~~

~~Principle 15: Sub-Custody~~

~~(1) Where authorised by a client or by law, a custodian may hold a digital asset for that client through another custodian (a "sub-custodian") if the sub-custodian is bound by the duties set out in Principle 13 above.~~

(2) Where a custodian holds a digital asset for a client through another custodian:

(a) If the sub-custodian enters into any insolvency proceeding, the custodian must seek to obtain control of the digital asset from the insolvency administrator, or to hold the asset with another sub-custodian;

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

Commentary

1. Principle 15(1) sets out the consequences of the insolvency of the custodian in a functional way rather than using legal concepts such as property or ownership. On the custodian's insolvency, assets it controls for clients as custodian are not part of the distributed estate. If a holder is not a custodian, any assets it controls will usually be part of its assets for distribution to its creditors. The effect of Principle 12(3) is that any agreement which has the three characteristics of a custody agreement set out in Principle 12(3) will attract the consequences in Principle 15(1) unless the agreement makes it clear that this is not the case.

2. Principle 15(2) sets out the consequences, where a digital asset is held through a sub-custodian (see Principle 13(4)) of the insolvency of a sub-custodian or a custodian.

Examples

Examples of custody

[description of 'pure' custody]

Custodial or Hosted Wallet

3. In a custodial or hosted wallet arrangement, users transfer digital assets to the wallets of a service provider, and that service provider holds the private keys of whichever wallet the digital asset is thereafter connected. Hosted wallets often appear in the context of trading platforms, where an intermediary facilitates trades of digital assets between users. Below are three examples of such

hosted wallet services. As will become evident, service providers often offer more than one kind of wallet service, allowing users to take advantage of both self-custody and custodial wallet solutions because the two different types of wallets serve different purposes.

Blockchain.com Trading Account

4. Blockchain.com separately offers what it terms a “Trading Account,” which is the functionality within the Wallet that enables a user to buy and hold all digital assets purchased with fiat currency through Blockchain.com (Section 18, Section 4.1). Blockchain.com holds all digital assets in a user’s Trading Account on trust by Blockchain.com, for the user’s benefit, on a custodial basis (Section 4.1). As a result, Blockchain.com is explicit in its terms that title to the digital assets in the Trading Account remains with the user and does not transfer to Blockchain.com (Section 4.1(a)). Further, Blockchain.com emphasises that digital assets in the trading account are not the property of Blockchain.com, and are not loaned to Blockchain.com (Section 4.1(b)). Blockchain.com also represents that it does not take secured loans using Trading Account digital assets as collateral (Section 4.1(b)). Blockchain.com segregates digital assets in the trading account from its own assets “by way of separate ledger accounting entries for customer and Blockchain.com Group accounts” although such digital assets may not be segregated “by blockchain address” (Section 4.1(d)). Some transactions initiated from a trading account occur off chain, and are noted only by accounting ledger entries by Blockchain.com. A transaction between a Private Key Wallet and a Trading Account, on the other hand, would occur on-chain, because of the self-custodial nature of the Wallet.

Coinbase Digital Asset Wallet

5. This is the original Coinbase product. The Digital Asset Wallet allows users “to store, track, transfer and manage [their] balances of Supported Digital Assets” (User Agreement Section 2.2). Coinbase stores the digital asset private keys associated with a user’s Digital Asset Wallet. Coinbase reserves the right to hold private keys associated with a user’s Digital Asset Wallet in a variety of ways – whether on the primary protocol those digital assets are associated with or not. In particular, Coinbase reserves the right to hold digital assets “across multiple protocols, such as layer two networks, alternative layer one networks, or side chains” and to transfer digital assets off the primary blockchain protocol and into shared blockchain addresses on different protocols (Section 2.5). The user is required to agree that “all forms of the same Digital Asset that are held and made available across multiple blockchain protocols may be treated as fungible and the equivalent of each other, without regard to (a) whether any form of such Digital Asset is wrapped or (b) the blockchain protocol on which any form of such Digital Asset is stored (Section 2.5).

6. Coinbase recently received some negative attention from filing a K-1 with the SEC that stated its belief that assets in the Digital Asset Wallets would form part of Coinbase’ bankruptcy estate in the event of a bankruptcy filing. Specifically, Coinbase’s K-1 stated “Because custodially held crypto assets may be considered to be the property of a bankruptcy estate, in the event of a bankruptcy, the crypto assets we hold in custody on behalf of our customers could be subject to bankruptcy proceedings and such customers could be treated as our general unsecured creditors” (Coinbase warns customers they may lose crypto if company goes bankrupt (nypost.com)). The public did not react favorably to this element of the K-1 filing, and in the wake of the bad press, Coinbase added Section 2.7 to its User Agreement, and in particular Section 2.7.2. In Section 2.7.2, Coinbase declares it is a securities intermediary under Article 8 of the UCC and that a Digital Asset Wallet is a securities account under Article 8, and therefore, users retain title to all digital assets in their wallets (section 2.7.1).

Coinbase Custody

7. Coinbase Custody is also a hosted wallet service. Coinbase Custody is aimed at institutions and institutional investors. Coinbase Custody requires a minimum balance of \$10 million USD and charges a setup fee of \$100,000 USD and a monthly basis points fee.

[description of an exchange]

[description of custody of a 'tethered' asset]

Examples of situation which are not custody

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

Self-Custody and/or Non-Custodial Third-Party Wallet.

9. Self-custody is when a user does not engage an intermediary to hold their keys on their behalf. Rather, a user holds private keys either using software solutions deployed directly on their own computer or mobile phone, or using cloud-based software-as-a-service non-custodial wallets. The two options are quite similar, as explained below, using MetaMask as the software example, and Blockchain.com as the software-as-a-service example.

MetaMask

10. MetaMask is open source software for self-custody of digital assets. To many, the term self-custody is a bit of a misnomer. MetaMask is just a wallet software, the same way your physical wallet is just your wallet, rather than a self-banking of cash. The MetaMask software, as open source software, is developed by "a global community of developers and designers." (About | MetaMask) The MetaMask software is compatible with a variety of hardware wallets. (How to blockchain wallet FAQs | MetaMask). When you use MetaMask, you create a wallet password and create a Secret Recovery Phrase, both of which must be kept secret. MetaMask then "stores the Secret Recovery Phrase, Passwords, and private keys in an encrypted format locally on the device where it's installed." (Id.) MetaMask is not an intermediary of any kind. Transactions conducted through MetaMask wallets are broadcast on-chain.

Coinbase Wallet

11. Coinbase Wallet is Coinbase, Inc.'s relatively new self-custody wallet. It functions like MetaMask and is offered to developers with an API for use in DApps.

12. Safeguarding of private keys. Another arrangement is where a business safeguards its client's private keys or provides software or hardware to facilitate the client's safekeeping its private keys. Depending on the features ~~of this service~~, the business providing the software or hardware may (or may not) have the ability to use the client's private keys and thus take control of the client's digital assets. However, this is not the purpose of ~~the service~~ this type of arrangement and typically the business will be prohibited from using the client's private keys for any purpose that has not been agreed by the client. The client still has control of the digital asset, and has the ability to change the control of the asset (using the terminology in Principle 6 (1)(a)(i)). This ~~service~~ business model is therefore not a custody service as defined in this ~~p~~ Principle, even though it is sometimes called "custody" by market participants. In contrast, where a business provides a custody service, its clients transfer their digital assets to addresses or private keys controlled by that business, or the business

acquires digital assets which it controls on behalf of the client. [A real world example of this situation is as follows:](#)

[Ledger Nano Wallet](#)

[13. The Ledger Nano Wallet generates private keys within the device, and then stores the keys there. This provides very secure cold wallet storage, by keeping the keys unconnected, and thus out of reach from online hackers and other threats, from the moment of generation until the moment of use. The software on the Ledger Nano hardware is not intermediated. No third party intermediary has access to the keys held on the Nano wallet.](#)

[14. When a user wants to transact with the keys held in a Ledger Nano wallet, they use Ledger Live to send, buy, or sell digital assets. Ledger Live is akin to a mobile phone app store. Ledger does not offer custody services itself, but rather, you can access other services, including some custodial trading wallets through Ledger Live.](#)

[Blockchain.com](#)

[15. The wallet offered by blockchain.com is a non-custodial wallet. The wallet is wallet software published by Blockchain Luxembourg S.A., that allows a user to “self-custody Digital Assets, organise network addresses, view transaction history and transact in Digital Assets” \(User Agreement Section 18\). When a user creates an account, the user confirms understanding that, not only does Blockchain.com not have access to the user’s private keys, but it also “never stores passwords and therefore cannot recover or reset \[a user’s\] password. If \[a user\] lose\[s\] access to \[their\] wallet, \[they\] must use \[their\] Secret Private Key Recovery Phrase to access \[their\] funds.” In the terms of service, the user agrees that they “are solely responsible for maintaining the security of \[their\] credentials” \(User Agreement Section 2.2\). This is because Blockchain.com never receives or stores any wallet password, any keys, network addresses or transaction history \(Section 3.4\(a\)\).](#)

[16. As explained by Blockchain.com: “Your Blockchain.com’s Private Key Wallet is non-custodial. This means that Blockchain.com does not hold those balances for you. When you sign up for a Blockchain.com Wallet, you’re creating an encrypted file that contains the information you will use to access your non-custodial crypto balance: your seed \(Secret Private Key Recovery Phrase\), private keys, and cryptocurrency addresses. The file is encrypted with your password, which we never store or have access to. You are solely responsible for the ownership and control of your private keys. As long as you keep your password and private keys secure, only you can ever access your Private Key Wallet and its non-custodial balance.” Technical differences between the Private Key Wallet and Trading Account – Blockchain Support Center. In other words, Blockchain.com keeps the users private key in an encrypted file in the cloud, but only the user can decrypt it with either their private key or their seed phrase, and when a password or seed phrase is used correctly, the file containing private keys is decrypted client side \(locally on the user’s computer\) such that Blockchain.com cannot intercept the keys and never knows how to access them. The only way Blockchain.com could access a user’s private keys in the self-custody wallet would be if Blockchain.com hacked its own software encryption. Further, Blockchain.com does not intermediate transactions from the Wallet. All transactions conducted using the Wallet are conducted directly on-chain. The key difference between Blockchain.com and MetaMask from a technical perspective is that Blockchain.com stores the encrypted file in the cloud, while MetaMask stores the encrypted file locally on the user’s computer. In other words, Blockchain.com Wallet is software-as-a-service, while MetaMask is software. Users of the software-as-a-service model, therefore, could find themselves in difficulty should Blockchain.com ever decide to stop providing the Wallet services.](#)

3.17. Agreement for a deposit account. A Fintech firm or a financial institution, such as a dealer, an exchange or a trading platform may incur an obligation to deliver a certain quantity of a given digital asset to a client because it has received the asset from the client or because it has acquired the asset on the primary or secondary market on behalf of the client. The firm or institution will maintain an account on which credits and debits of a particular digital asset are recorded from time

to time so that the account balance evidences at any time the quantity of such digital asset the firm or institution is obliged to deliver to the client (or, as the case may be, may claim from the client). For each digital asset, such an account operates in the same way as a current account in a fiat currency. The investor does not have control of digital assets; she merely has an unsecured personal claim against the account provider. If the account provider becomes bankrupt, the claim for delivery of a digital asset is likely to be converted into a (fiat) money claim and will rank *pari passu* with the claims of all other unsecured creditors. [Please note that if the digital asset is not fungible, the relevant claim is for delivery of a specific asset rather than for a generic quantity of a particular digital asset. This, however, should not alter the legal characterisation of the obligation as a personal right or its treatment as an unsecured claim in the bankruptcy of the obligee.]

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

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

Continued Issues Paper

101. The change made to Principle 15(1)(a) was introduced during DC9 to ensure that the Principle had a broader application. This is an alternative to obtaining direct control. Additional Commentary for this might be introduced into the draft after the WG meeting.

102. Several additional examples of real-world businesses have been added to the Commentary for this Principle in order to illustrate the types of situations which might be considered custody, as defined by the Principles, and those which are not custody. For the final version of the Principles and Commentary, the names of these companies will be removed and a more neutral Commentary will be prepared. The present inclusion of names is for the purposes of aiding the WGs understanding of the Principles and their application to real companies.

103. With regard to DAOs, comments from a representative of Turkey and a representative of Luxembourg from the Steering Committee make the point that in theory, there is usually some degree of centralisation which could make liability possible. A comment from a representative of Switzerland notes that true DeFi are of a non-custodial nature.

SECTION VI: ~~COLLATERAL~~SECURED TRANSACTIONS

Principle 16: ~~Collateral Transactions~~Secured transactions: General

⌘

(1) Digital assets ~~are eligible to~~can be the subject of security rights.

Commentary

~~(a) — References in secured transactions laws to movable assets, personal property or any similar notion should be understood to include digital assets.~~

Commentary

1. Secured transactions regimes should enable the use of anything that is a movable asset and not necessarily property in the strict sense as collateral. Digital assets, whether or not capable of being ~~controlled or~~ maintained by a custodian ~~as collateral~~could thus be made subject to a security right. This approach allows prospective secured creditors to decide for themselves which of the digital assets of ~~a loan applicant~~ have any collateral value. This Principle, however, builds on the Principle 2(1) stating that law should provide that digital assets (as defined in Principle 2(2)) may be the subject of proprietary rights. The inclusion of Principle 16~~(1)~~ allows the explanation of this aspect in the context of secured transactions. As is explained in Principle 4, other law determines whether a digital asset embodies a right in another (tethered/linked) asset—or whether a security right over that other asset is validly created.

2. This Section applies to transactions under which a security right in a digital asset is granted to a secured creditor to secure the performance of any existing, future or contingent obligations of the grantor or another person. In this Section, “secured transactions” should be understood to include various types of “security rights”, such as pledges, charges, or security assignments. It may also cover outright transfers where those might be used with respect to certain types of digital assets: whether “secured transactions” includes such transfers will depend on domestic secured transactions law. [For example, the UNCITRAL Model Law and some domestic secured transactions laws apply to outright transfers of receivables. The Geneva Securities Convention covers collateral transactions that are created by the grant of an interest in intermediated securities in the form of security interests and title transfer collateral agreements. Some domestic laws provide for fiduciary transfers of ownership that transfer “ownership” of the asset to the creditor with the sole purpose of securing an obligation.] The Principles in this section are not intended to interfere with domestic conception of security right or domestic security law, except to the extent that such law should be changed to deal specifically with security over digital assets. However, it is important that secured transactions law should be coordinated with the generally applicable rules governing outright transfers of digital assets.

Illustration

3. The civil law of a State defines ‘things’ and provides that a security right may be taken over ‘things’. It is unclear whether that State’s definition of “things” includes digital assets. Principle 16 makes it clear that this should be the case.

[Notes [this section to be aligned with the commentary on other principles]

~~Illustrations~~

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

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

Notes

~~2.4.~~ Some secured transactions regimes may enable the use of any movable property as collateral, while others specify the types of property that may be encumbered (e.g., equipment, but not inventory of a business, may be subject to an enterprise charge under some laws). The former, ~~whether statutory or judge-made,~~ may define a security right as a “property right in a movable asset”, without defining “movable asset”.¹⁴ Applicable Other law defines what constitutes a movable asset. Some laws allow the creation of an interest with respect to anything that can be traded, including intangible assets.¹⁵ Although actions, claims or rights may be listed as an example of an ~~incorporeal~~ intangible 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~~ intangible asset, including digital assets. However, an explicit statutory treatment would in this case provide greater legal certainty.]

Commentary

~~(2) — The law should provide distinct rules in relation to creation of a security right and effectiveness against third parties for 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.~~

~~(3) — Separation of digital assets from the general category of intangible assets would enable the State to consider specific approaches, such as third-party effectiveness by control.~~

Commentary

~~5.~~ Digital assets may fall under different types of collateral (e.g., securities, bank accounts, etc.) defined in the secured transactions laws. In adopting these Principles, a State is likely to amend existing secured transactions legislation by including special rules for digital assets as set out in this Section. In doing so, the asset to which these special rules apply will have to be defined, using the definition in Principle 2(2) of these Principles.

~~3.6.~~ Depending on their characteristics, before a State’s law is amended to provide for a specific type of collateral – digital assets, they ~~may be treated as~~ (including digital assets linked to another asset) may fall within specific categories in the domestic law of a State, such as securities, funds credited to bank accounts, negotiable documents/instruments,⁷ (if the State recognizes electronic documents and instruments⁷) or may fall under the ~~the~~ residual category of intangible assets/general intangibles. As a consequence, the secured transactions rules specific to that type of asset will apply. A number of these rules have been designed with reference to the specific nature of an asset or the

¹⁴ — This is the case of the UNCITRAL Model Law that also takes a comprehensive approach with the aim to cover all types of movable assets except those explicitly excluded (see article 1(3)). See also R. Goode, L. Gullifer, *Goode and Gullifer on Legal Problems of Credit and Security*, (Sweet & Maxwell, 6th edn, 2018) 39; G. McCormack, R. Bork, *Security rights and the European Insolvency Regulation* (Intersentia, 2017) 313.

¹⁵ — 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.

structure of the system in which it is transacted, which could cause challenges in determining how those rules are to be applied to security rights in digital assets. ~~If a digital asset tethered to some real-world asset is recognized under some other law as a negotiable document~~For instance, the ~~creation and law applicable to the~~ third-party effectiveness ~~and priority~~ of a security right in ~~the digital asset would extend to non-intermediated equity securities is~~ the ~~real-world asset. Otherwise, law of the creation and third-party effectiveness of a security right would cover~~location of the ~~digital asset only~~ issuer, under Article 100 of the UNCITRAL Model Law. However, many digital assets do not have an issuer, or its location can't be readily determined.

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

8. The Principles in this Section address certain aspects of third party effectiveness, priority and enforcement, but there will be many aspects of secured transactions that are governed by other law (that is, domestic law that is not Principles law). The rules determining the applicable law are set out in Principle 4.

Illustration

~~Illustrations~~

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

(42) If a digital asset is linked to another asset, the legal effect on that other asset of the creation of a security right in that digital asset is a matter for other law and is not covered in these Principles.

(53) If a digital asset is linked to another asset, the legal effect on that other asset of a security right in that digital asset being made effective against third parties is a matter for other law and is not covered in these principles.

Commentary

10. Paragraphs (4) and (5) reflect Principle 4 which provides that the existence of, requirements for and legal consequences of any link between a digital asset and another asset are a matter for other law. If a digital asset linked to some real-world asset is recognised under other law, for instance, as a negotiable document, the creation and third-party effectiveness of a security right in the digital asset would extend to the real-world asset. Otherwise, a security right would extend to the digital asset only.

Illustration

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

Continued Issues Paper

104. The Commentary for this Principle has been expanded in order to clarify to readers the meaning of 'Secured Transaction' under this Principle and the types of transactions to which this Principle applies and does not apply.

105. There are similarities between Principle 16(1) and Principle 3(1) which states that 'Digital assets can be the subject of proprietary rights', as, in theory, if digital assets can be the subject of proprietary rights, they can also be the subject of security rights. However, the Drafting Committee has proposed that it would be beneficial to emphasise this point in this section.

106. Regarding the deletion of subparagraphs (2) and (3), it was suggested at the Drafting Committee that in relation to third party effectiveness, the distinct rule in Principle 17 was a substantive Principle and did not require any additional explanation in Principle 16. One paragraph has been moved to the Commentary and other deleted items are also explained further in the Commentary.

107. Several comments from representatives in the Steering Committee mentioned title transfer arrangements rather than security arrangement being the norm with digital assets. This has been further explained in Paragraph 2 of the Commentary.

108. The changes to the parts referring to linked assets in this Principle make this Principle consistent with Principle 4. Some parts of the Commentary have also been adjusted for this.

109. It is noted that this Principle applies to transactions which are secured transactions under a particular domestic law, and that the Principles are not advocating recharacterisation of title transfer devices if they are not recharacterised in a national law. It is not the function of these principles to advocate for a comprehensive secured transactions law reform along the lines of the functional approach.

110. A representative of Iran from the Steering Committee has noted:

No idea about examples of best practices of the security right perfection in collateral transactions involving digital assets. But, it is necessary to pay attention to a few points. In traditional banking, customers are given credit points based on their past trading behavior and financial status. This is almost impossible in the crypto loan market because wallets are created anonymously, and anyone can make as many wallets as they want. Unlike traditional collateral, such as cars or homes, whose value are more predictable and do not change dramatically in the short term, collateral in the world of digital currencies, such as NFT or cryptocurrencies, can fluctuate widely. Therefore, lending platforms need to have strong collateral valuation systems that can estimate the market value of any asset at any time. On the other hand, lending platforms can create something similar to the concept of risk-weighted assets (RWAs) in traditional banking. Additionally, because transfers in crypto assets are irreversible and hard to trace, these assets seem risky to be used as collateral if the debtor has the possibility of transferring them at any time. Moreover, there is a fear that security interests will continue to burden the cryptocurrency that has passed into the hands of a party whose property serves as security for a blanket lien. Nonetheless, solutions exist. The main idea to facilitate digital assets as collateral in secured lending is to create a whole new category for them and amend the laws to create a more suitable framework. This entails that a definition of digital assets must be added and amendments to allow creditors to perfect their security interests in digital assets through control.

111. This is similar to the approach taken by this section of the Principles.

Principle 17: Control as a ~~Method of Achieving Third-Party Effectiveness~~ method of achieving third party effectiveness

(1) ~~The law should provide for control as a mechanism~~ A security right in a digital asset can be made effective against third parties by control of the digital asset as set out in Principle 6(1) if one of the following requirements is fulfilled:

- (a) the secured creditor controls the digital asset; or
- (b) a custodian [holds] [controls] the digital asset on behalf of the secured creditor.

[(2) A security right in a digital asset is not made effective against third parties if the secured creditor shares an ability for the purposes of Principle 6(1)(a) with the grantor in such a way that the grantor can exercise that ability without the need for the secured creditor to exercise that ability.]

(4) If a digital asset falls under a type of an asset for which the secured transactions law has provided one or more methods to achieve third-party effectiveness of, a security right in a digital asset may be made effective against third parties by one of those methods.

Commentary

~~(2) — The requirements to achieve third party effectiveness of a security right by control may be:~~

~~(i) — those set out in Principle 6 (1)(a)(i) and (iii) (“positive control”) or~~

~~(ii) — that set out in Principle 6 (1)(a)(ii) (“negative control”) or~~

~~(iii) — those set out in Principle 6(1)(a)(i), (ii) and (iii) (“negative and positive control”).~~

~~(3) — It is sufficient to satisfy the requirement of control if~~

~~(a) — a custodian holds a digital asset on behalf of the secured creditor or~~

~~(b) — a custodian is itself the secured creditor.~~

~~[(4) — The law should specify which (if any) of its existing special rules govern the third party effectiveness of security rights in digital assets.]~~

Commentary

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

2. ~~2.~~ — While in some States registration of a notice would generally render a security right in most (or all) types of assets effective against third parties, registrations are not commonly

effectuated in the crypto-lending market, leaving some credit risk in the transaction. Furthermore, in States that do not have a registration system, market participants may not be aware of the existing requirements for third-party effectiveness or such requirements may be an obstacle to the practices.

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

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

5. ~~5.~~—Regimes governing security rights in certain types of assets have been amended reflecting the emerging industry practice (e.g., book entries to securities accounts in which financial collateral is held). The emerging practices in “crypto-lending” do not rely on registration and other traditional methods of achieving third-party effectiveness. ~~States~~ A State should incorporate “control” as defined in Principle ~~×6~~ in ~~their~~ its secured transactions laws to allow secured creditors to make their security right in digital assets effective ~~ness~~ against third parties. Incorporation of control may affect the structure of its priority rules, which is explored below in Principle ~~E18~~ on priority as well as facilitate enforcement, which is explored in Principle 19.

6. ~~6.~~—There are four situations in which control may be ~~deployed~~ used to make the security right effective against third parties. First, the existing rules on control in the relevant secured transactions regime may ~~be used~~ apply if the digital asset qualifies as a particular type of asset (e.g., bank account). Second, the secured creditor may acquire the requisite powers prescribed in Principle ~~×6~~. Third, the secured creditor may share these powers with other parties, which would also constitute control under Principle ~~×6~~. Fourth, a party that is currently in control (e.g., a custodian) may agree to exercise those powers on behalf of the secured creditor.

7. A State should include ~~a~~ the specific definition of control in Principle 6 in its secured transactions law (or refer to such a definition included elsewhere in ~~the~~ its law relating to digital assets ~~law~~) to achieve third-party effectiveness ~~conditioned on the secured of a security right in a digital asset.~~ “Control” within this definition exists when a secured creditor acquires a set of

abilities with respect to the digital asset. ~~This project has developed Principle X on control~~ 17 (1) (in conjunction with Principle 6(3)) provides that ~~is suitable to achieve third-party effectiveness of security rights over any digital assets by transferring the powers specified therein to~~ the secured creditor. ~~The secured creditor~~ may exercise the requisite powers directly, through ~~an agent~~ a third party custodian or in cooperation with other parties, such as in (a multi-sig) arrangement.

8. ~~8.~~ Although specific rules may have already been provided in some States prescribing control for some assets, such as electronic transferable records, ~~States~~ a State should ensure that the existing criteria are sufficient to accommodate collateralization of these records issued and transferred ~~in~~ through any type of technology, including blockchain. For instance, the UNCITRAL Model Law on Electronic Transferable Records in Article 11 provides for control requiring that an identified person acquires exclusive control by a reliable method. States implementing this Model Law should consider incorporating the criteria establishing control under Principle ~~X6~~ for transfers of “electronic transferable records”, including achieving third-party effectiveness of a security right.

Illustrations

Illustrations

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

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

Continued Issues Paper

112. Principle 17 underwent changes to improve clarity and consistency with the other Principles. It was discussed in detail at DC9, where it was agreed that instead of specifications on 'negative' and 'positive' control, a reference to Principle 6(1) on Control was included to better specify the notion of control used, particularly noting its factual nature.

113. References in the Commentary to 'mechanism' have been changed to 'method' for consistency with the Principle. The Commentary of this Principle explains how the notion of control, as defined in the Principles, may be applicable in different jurisdictions. Some changes have also been introduced to make the Commentary technologically neutral.

114. Because of the mentioned specific use of 'control' and a definition of 'hold' provided in Principle 12(2)(b), both options are presented in square brackets in Principle 17(1)(b) for the Working Group's consideration, particularly, taking into account sub-custody.

115. A paragraph on the control of the secured creditor shared with the grantor was added for further discussions during the Fifth Working Group.

Principle 18: Priority of ~~Security Rights~~security rights in ~~Digital Assets~~digital assets

- (1) ~~{The law should provide that}~~~~[W][w]here~~ Where a security right in a digital asset has been made effective against third parties by ~~through~~ control, the security right ~~should have~~has priority over a security right, in the digital asset, of a ~~person~~secured creditor that does not have control.
- (2) **Where more than one security right in the same digital asset has been made effective against third parties by control, ~~priority should be based on the temporal order of obtaining control.~~the security rights rank among themselves according to the time when the secured creditor obtains control.**

Commentary

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

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

3. ~~3.~~—Similar concepts would apply to a security right in a digital asset. Where one secured creditor made its security right effective against third parties by registration or another ~~mechanism recognized~~method recognised by the applicable law and another secured creditor made its security right effective by control (~~as defined under~~pursuant to Principle ~~¥17~~), the latter would have priority even if it took the steps to obtain control after the former registered a notice relating to a security right in the registry or otherwise made it effective against third parties. This approach is consistent with the secured transactions rules, including the UNCITRAL Model Law and the relevant provisions of the Geneva Securities Convention that give priority to secured creditors that acquired some form of control over the collateral. A different approach would create distinctions between non-digital assets, such as funds held in deposit accounts, and their digital functional equivalents, such as the CBDC. Furthermore, Principle 9(~~41~~) generally cuts off any conflicting proprietary claims. The secured creditor acquiring control is expected to satisfy the other requirements to qualify as an innocent acquirer.

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

~~5.~~—Under Section VI, more

5. More than one secured creditor can obtain control (or share such ability) over the digital assets, which includes making their security right effective against third parties. As a result, there

should be a rule to determine the priority between the multiple secured creditors based on the temporal order of obtaining control. [In those circumstances, other law would generally permit secured creditors to alter the statutory ranking of priorities through a subordination and/or intercreditor agreement.](#)

Illustration

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

Continued Issues Paper

116. The changes made to Principle 18(1) are to provide more clarity to the draft. At DC5, the word 'person' was replaced with 'secured creditor'.

117. In Principle 18(2), consideration was given to using language with regard to priority rights which was similarly found in the Geneva Securities Convention (I.e., 'to the time of occurrence' of the). However, it was decided by the DC to use even simpler language to explain priority rights with respect to digital assets.

118. With regard to Principle 18(2), a representative of the United States and a representative from the Netherlands on the Steering Committee queried whether it was possible that two secured parties could both have control, saying that in the case of shared control, there would be an agreement between secured creditors. On a similar point, a representative of Luxembourg approved of this Principle noting that where there were two lenders taking control, the first was likely to act as security trustee for the second.

119. To address these comments, an additional sentence has been included in the Commentary.

Principle 19: Effective ~~E~~enforcement of ~~Security Rights~~ security rights in ~~Digital Assets~~ digital assets

(1) ~~The law should allow~~ A secured ~~creditors~~ creditor should be able to enforce ~~their~~ its security rights in ~~a digital assets in a simple~~ asset simply and ~~quick~~ manner. ~~To that end,~~ quickly, ~~without~~ the law ~~should not impose~~ imposition of undue formalities or requirements that would make the enforcement process cumbersome.

(2) The interests of ~~third parties, particularly~~ custodians ~~and other intermediaries~~ should be protected: ~~on the enforcement of a security right in a digital asset.~~

(3) ~~—Given~~ There should not be any requirements [as a matter of Principles law] inconsistent with the ~~nature of~~ automatic enforcement of a security right in a digital assets, ~~asset, except to~~ the law ~~should recognize~~ extent that ~~enforcement actions may be taken automatically and~~ it is necessary to ~~ensure~~ that ~~some requirements for~~ the enforcement, ~~such as to provide a notification of disposal, should not apply.~~ is carried out in a commercially reasonable manner.

Commentary

Commentary

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

~~2. —The law~~

2. [Principle 19 does not prescribe particular enforcement methods for security rights in digital assets: it merely provides guidance to States as to how existing enforcement rules should apply in relation to such security rights.](#) The law of a State should not preclude secured creditors from exercising remedies that may exist under other laws or have been provided for in the security agreement. When digital assets become widely used in securities transactions, derivatives, and similar financial structures, States should ensure that close-out netting is available to parties to such transactions.

3. ~~3. —~~ All enforcement actions, including disposal, collection of payment (if [the right to payment of a](#) monetary obligation is the ~~main characteristic of~~ asset to which a digital asset [is effectively linked](#)) and acceptance of the collateral, in full or partial satisfaction of the secured obligation, should be available: [in relation to security rights in digital assets](#). In enforcing their rights, secured creditors must proceed in a commercially reasonable manner and satisfy certain conditions that balance the interest of affected third parties. ~~The~~ [In some cases, the](#) inherent design of the digital asset may prevent ~~exercising~~ [the exercise of](#) certain enforcement rights. General rules governing enforcement, typically included in international standards on secured transactions appear to be flexible enough to accommodate the expectation of digital assets lenders and other relevant parties. However, States should take into account ~~several~~ [a number of](#) considerations, [including the matters set out in Principle 19](#).

~~4. —~~ First, enforcement rules empower a secured creditor to take a post-default action. Generally, a secured creditor or its agent would take some action, such as repossessing the collateral or instructing the debtor of a receivable to pay to a different bank account. While the rules focus on

~~post default actions taken by secured creditors, they should not render a “pre-programmed action” that occurs automatically, such as causing liquidation of the digital asset when the collateral-to-loan ratio falls under a specified threshold ineffective. See Illustration 1 above for the automated enforcement action occurring upon reaching a specific collateral-to-value limit.~~

~~5. — Second, secured~~

~~4. The method used to make the security right effective against third parties can have an impact on the ability to enforce security rights. Control is a facilitator of enforcement upon default, so that if a security right is made effective against third parties by control, enforcement by the secured creditor is likely to be reasonably straightforward. However, if a security right in a digital asset is made effective against third parties by registration rather than by control, it is likely to be difficult in practice for the secured creditor to enforce against that asset without the cooperation of the grantor, since the grantor retains control of the asset. Thus, the secured creditor might need to obtain a court order, after default, to obtain control if the grantor refuses to transfer it. This situation would be analogous to the grantor refusing to surrender possession of a tangible asset.~~

~~4.5. Secured transactions laws typically balance the interests of affected parties by imposing certain requirements on secured creditors when enforcing a security right, such as to provide notifications. However, to affected parties. These types of requirement could, potentially, fall into the category of requirements referred to in Principle 19(1) as formalities or requirements that make the enforcement process cumbersome. However, secured transactions laws also, typically, provide that under certain situations these requirements may will not apply. For instance, Article 78(8) of the UNCITRAL Model Law provides for exceptions from the requirement to provide a notification when the asset may speedily decline in value or is sold on a recognised market. These kinds of exceptions should, arguably, apply to many, though not all, digital assets (e.g., Bitcoin may speedily decline in value while stablecoins may not, and some NFTs may already trade on recognised markets while others do not). Enforcement provisions in secured transactions laws may not need to be changed to accommodate digital assets as in accordance with Principle 19(1) if these exceptions were generally crafted broadly to accommodate future developments. For those digital assets Some States also have bespoke enforcement procedures for specific types of assets that qualify as intermediated securities (e.g., upon their credit to a securities account), which do not include any notification requirements may not apply at all.¹⁶ (for example, in relation to intermediated securities, Article 33 of the Geneva Securities Convention provides for enforcement by sale or appropriation of securities without notice). It would be consistent with Principle 19(1) for a State to provide for an analogous enforcement procedure in relation to security rights over digital assets, particularly those which are similar to the types of assets for which such enforcement procedures already exist.~~

~~6. — Third, States should be mindful~~

~~6. If a custodian holds the digital asset on behalf of some limitations on the enforcement rights. One such limitation relates to the mechanism used to make the security right effective against third parties, which can have an impact grantor, extra-judicial enforcement will entail action by that custodian on the ability to enforce security rights. For instance, the law should provide that instructions of the secured creditor. An intermediary will be unwilling to follow those instructions if the secured creditor registered a notice, secured creditors may not be able to extra-judicially enforce their security rights in digital assets held with custodians. This approach mirrors the rules that protect is unknown and many secured transactions laws include provisions protecting intermediaries, such as banks against “unknown” third party creditors. Extra-judicial enforcement is available when the in this situation. For example, Article 82(4) of the UNCITRAL Model Law provides that, in relation to a security right over a bank account, extra-judicial enforcement is only available when the bank has agreed to act on the instructions of the secured creditor. Principle 19(2) provides for the protection of the interests of third parties on the enforcement of a security right in a digital asset. In the context discussed in this paragraph this would entail the restriction of extra-judicial~~

¹⁶ — see Article 33(3)(a) of the Geneva Securities Convention.

enforcement of a security right made effective against third parties by registration to the situation where the secured creditor holds a power to instruct the custodian to change control of a digital asset or has entered into a control agreement with the custodian (see Article 82(4) of the UNCITRAL Model Law). In other words, control is the facilitator of enforcement upon

~~5.7.~~ General enforcement rules empower a secured creditor to take a post-default action. In a typical secured transaction not involving digital assets, a secured creditor or its agent would take some action, such as repossessing the collateral or instructing the debtor of a receivable to pay to a different bank account. In relation to digital assets, while the rules focus on post-default actions taken by secured creditors, Principle 19(3) provides that they should not render a “pre-programmed action” that occurs automatically ineffective and that requirements in the general law that are inconsistent with such automatic enforcement should not apply in relation to digital assets, except to the extent that it is necessary to ensure that the enforcement is carried out in a commercially reasonable fashion and that the secured creditor is obliged to distribute any surplus value to the competing claimant or the grantor entitled to it. An example of automatic enforcement is where liquidation of a digital asset occurs automatically when the collateral-to-loan ratio falls under a specified threshold. This would be an enforcement of a security right if the fall in the ratio is a default under the terms of the security agreement. However, the law should provide for such enforcement to be carried out in a commercially reasonable manner. [See Illustration [] for the automated enforcement action occurring upon reaching a specific collateral-to-value limit.]

8. There should not be any requirements [as a matter of Principles law] inconsistent with the automatic enforcement of a security right in a digital asset, except to the extent that it is necessary to ensure that the enforcement is carried out in a commercially reasonable manner.

Illustrations

~~7. Fourth, collateral may need to be disposed of in a public/private sale that proceeds differently from selling tangible collateral, for instance. Smart contracts may execute successive auctions of the encumbered digital assets until the secured obligation is satisfied. Thus, the collateral may not be sold in its entirety, and any collateral in excess of the amount necessary to satisfy the secured obligation is returned to the borrower. The law should not preclude such automatic liquidation of the collateral or impose requirements before each of the successive auctions can proceed.~~

Illustration

~~6.9.~~ A security right was made effective against third parties by control where the secured creditor is one of the three parties to a multi-signature arrangement. While the grantor is also a party to this arrangement, the third person acts on behalf of the secured creditor. An action of two parties is required to cause a transfer of control. Upon default, the multi-signature arrangement is triggered, and the encumbered digital asset is transferred under the “sole” control of the secured creditor resulting in the acceptance of the collateral in satisfaction of the secured obligation or enabling a foreclosure sale.

~~7.10.~~ Upon default, the ability of the secured creditor to dispose of the digital asset in a public auction may be affected by the design of the digital asset that may preclude its transfer out of the system in which it was issued and trades.

Continued Issues Paper:

120. Principle 19 has been redrafted with a more passive approach so as to better suit the style of the Principles whereby it notes that formalities and requirements should be kept to a minimum. Additionally, several changes proposed were also discussed at the Workshop on Issues related to Enforcement in Digital Assets held on 10 June 2022, DC8, and DC9.

121. Particularly, the element of a 'commercially reasonable manner' in para. 3 was added in a view of Article 79 of the UNCITRAL Model Law on Secured Transactions brought up during the mentioned workshop. Additional Commentary has also been added to further explain this point.

122. Two issues which have been considered include:

- a. how is the surplus value preserved for other creditors (that is a security right specific issue but it is likely to be already dealt with in other law and is not an issue that relates specifically to Digital Assets). It is noted that many jurisdictions require notice to other interested parties before a security right is enforced (because of the potential right in any surplus value); and
- b. how does enforcement work when digital assets are held through a custodian.

123. Apart from drafting improvements, the Commentary was expanded with explanations on potential impediments for enforcement related to the method of achieving third-party effectiveness, protection of third parties, and automated enforcement instances also presented at the workshop. More illustrations on commercial reasonableness will be included in the Commentary ahead of the Working Group's next session.

124. On this matter, representatives of Luxembourg and the Netherlands from the Steering Committee has noted:

Luxembourg:

I am not sure whether that Principle is feasible and encourage rethinking. Automatic enforcement may entail that, as part of the Smart Contract, there is an embedded right to retransfer the asset. That would undermine the trust in the functioning of the Smart Contract as there must be some mechanism to triggers this retransfer. Sometimes in the future we could envision that the Smart Contract may have some technical links to a court, and this link trigger the retransfer, but for lack of standardization and many other reasons I do not see this to happen anytime soon. In this case, humans will trigger the retransfer, and that brings the human factor back into a system designed to erase this human factor.

The Netherlands:

I do not see the need for explicit further exceptions as any exceptions should rather follow from the general rules regarding property and security rights. Where a specific exception is needed, that indicates that there should also be a special rule for property remedies in general.

125. It is noted that this is a general principle that would disapply certain requirements as explained in the Commentary, such as on notifications. A State would not need to enact this principle into its own law, but rather examine which provisions of the existing law might provide an impediment to an automatic enforcement action where appropriate.

SECTION VII: ENFORCEMENT

Principle 20: Enforcement

Procedural law should apply to digital assets, with any modifications necessary because of the distinctive features of digital assets.

Commentary

1. This Principle makes it clear that ordinary procedural law will generally apply to any court proceedings involving digital assets or any procedures for the enforcement of court orders involving digital assets. However, depending on the content of the procedural law of a particular State, some modifications may be required in order to take account of the distinctive features of digital assets.
2. Examples of possible modifications are:

Continued Issues Paper:

126. A Special Workshop on Issues Related to Enforcement in Digital Assets took place as a side event to the 101st Session of the UNIDROIT Governing Council in Rome and on Zoom on 10 June 2022. The Workshop was attended by Members of the UNIDROIT Governing Council, the UNIDROIT Working Group on Digital Assets and Private Law, the UNIDROIT Working Group on Best Practices in the Field of Effective Enforcement, as well as Members of the Steering Committee of the Working Group on Digital Assets. A summary Report of this Workshop is found in Annex 2 of this document. See <https://www.unidroit.org/workshop-on-issues-related-to-enforcement-in-digital-assets/>

127. The current version of the Enforcement Principle is the result of the deliberations at this workshop, and generally discussion between the two UNIDROIT Working Groups on this matter. The drafting is not final, and is intended only to form the basis of discussion at the WG.

128. Several open questions remain to be discussed. The WG is invited to provide input on the extent to which procedural law should be referenced in this Principle, given that practical limitations are often a big impediment for enforcement where the object is a digital asset.

129. It is noted that some aspects of enforcement are also covered in Principle 21(2)(c) which refers to the insolvency law of the forum with respect to enforcement of any remedies. Additionally, the principles on secured transactions (Principle 19 in particular) also concerns enforcement, but only in the context of security rights, and does not consider the enforcement of rights of holders or person digital assets.

SECTION VIII: INSOLVENCY

Principle ~~20~~¹: Effect of Insolvency on Proprietary [and Security] Rights in Digital Assets

~~(1)~~ **(1)** The law should provide that rights and interests that have become effective against third parties under Principle 9 (innocent acquirer~~er~~^{acquisition} rule) or Principle 17 (control as a method of third party effectiveness of security rights) are effective against the insolvency administrator and creditors in any insolvency proceeding.

(2) Paragraph (1) does not affect the application of any substantive or procedural rule of law applicable by virtue of an insolvency proceeding, such as any rule relating to:

(a) the ranking of categories of claims;

(b) the avoidance of a transaction as a preference or a transfer in fraud of creditors; or

(c) the enforcement of rights to property that is under the control or supervision of the insolvency administrator.~~;~~

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

~~(2) — The priority of a security right in digital assets established under the applicable law should be the same, except if, pursuant to insolvency law, another claim is given priority.~~

~~(3) — Secured creditors should be entitled to claim the value of encumbered digital assets.~~

Commentary

1. ~~1.~~ — The insolvency law should recognise the third-party effectiveness and priority of a security right and should not impair it for the sole reason that the collateral is a digital asset. The insolvency law should not impose any further requirement to establish or maintain the third-party effectiveness of a security right established prior to the insolvency proceedings.¹⁷

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

3. ~~3.~~ — Determining whether, and to what extent, a secured creditor is actually secured and may claim the value of its security right, requires valuation of the encumbered digital asset. Insolvency law may require/allow valuation of an encumbered asset pursuant to a pre-petition agreement of the parties, by the insolvency representative or by the court on the basis of evidence, including market considerations and expert testimony, taking into account the purpose of the valuation. The established insolvency law mechanisms for ascertaining the value of the asset may

¹⁷ See Art. 11(2) of the Geneva Securities Convention.

reflect either the going concern value or liquidation value. The relevant valuation date is crucial. This means that there may be a need for an ongoing valuation at different stages of the insolvency proceedings in order to determine the value of the encumbered asset itself, including facilitating the distribution of the proceeds of sale of the encumbered asset. Alternatively, upon commencement, the encumbered asset is valued and the amount of the secured portion of the creditor's claim is determined immediately, remaining unaffected in the course of the insolvency proceedings. In order to provide adequate protection of the security right in a digital asset in the insolvency proceedings and preserve the value of a creditor's security right, the valuation of the encumbered asset should take into account the high volatility and sharp fluctuations in value of many digital assets.

4. ~~4.~~ Valuation of assets affects recovery of secured creditors in an insolvency proceeding. It also impacts other aspects of secured transactions, including determination of the amount to be lent and distribution of proceeds upon disposition of the collateral. Insolvency laws do not provide specific guidance on the valuation method to be used, such as the "going concern value" or the "liquidation value". Currently, there are no standardized valuation approaches which creates uncertainty for secured creditors as to the value they may be able to receive. Given these challenges, it might be useful to explore and assess whether and how the existing valuation standards and methods apply to digital assets,¹⁸ focusing on the rights of secured creditors in insolvency. This may be particularly necessary for digital assets that do not have a value that may be readily established for instance through a secondary market. Such assets may include some NFTs and utility tokens, the value of which is not necessarily determined by supply and demand and thus, may require different ways to measure the value; for instance, by comparing them to similar ones. Valuation of "digital twins" may present peculiar challenges as well. The international standards could offer guidance as to which valuation approaches and methods to apply to digital assets, in accordance with their classification. On the contrary, valuation of digital assets, such as CBDCs, stablecoins, and other virtual currencies might be more straightforward but it could still benefit from further guidance.

5. ~~5.~~ Considering the diversity of rights and obligations associated with digital assets, the choice of the valuation approach may highly depend on the classification of the digital asset and its intended purpose. Besides, different valuation approaches may provide different results as the inputs used may vary. In specific circumstances involving certain digital assets, one valuation approach may be more appropriate than the others. Methodologies for the valuation of digital assets started to emerge, drawing on those applicable to intellectual property.¹⁹ This is particularly relevant for those digital assets linked to an intellectual property right (e.g. NFTs associated with art).

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

7. ~~7.~~ A further issue concerns whether valuation, and consequently distribution, should take place in fiat or virtual currency. For instance, in an insolvency scenario where digital assets are

¹⁸ Relevant international standards would include the *International Valuation Standards (IVS)* produced by the International Valuation Standards Council (IVSC), and the *International Financial Reporting Standards (IFRS)* developed by the International Financial Reporting Standards (IFRS) Foundation mainly through its standard-setting body, the International Accounting Standards Board (IASB).

¹⁹ A few reports on the analysis of suitable valuation approaches and standards for crypto-assets have been recently developed. Besides, there are discussions within the international valuation organisations to include digital assets in their scope; European Financial Reporting Advisory Group (EFRAG), *Accounting for Crypto-Assets (Liabilities): Holder and Issuer Perspective* (July 2020); Chartered Business Valuators (CBV) Institute, *Decrypting Crypto: An Introduction to Cryptoassets and a Study of Select Valuation Approaches* (2019); PWC, *In depth A look at current financial reporting issues, Cryptographic assets and related transactions: accounting considerations under IFRS* (No. 2019-05, December 2019).

valued and converted to fiat currency, creditors may receive the cash value of the assets, but would lose any future appreciation that the digital assets might accrue.

Illustrations

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

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

Continued Issues Paper:

130. Alternative 1 from the two drafting options was chosen for Principle 21 at DC9. Alternative 1 follows the model of the Geneva Securities Convention and was thought to be better suited for these Principles by the Drafting Committee. The Working Group is invited to provide feedback on this choice.

131. It is noted that in light of the choice of Alternative 1, the Commentary needs to be amended. This will be actioned ahead of the next session of the WG, as presently, it mostly relates to security rights, which were the main subject of Alternative 2.

132. There are several comments from representatives in the Steering Committee about this. In particular, a representative from Luxembourg notes that:

The insolvency principle is currently focusing on protecting the holders of security rights, which is of course important. Yet the largest problem in an insolvency where digital assets are involved is how the administrator can get control of the digital assets to which there are no security rights or even know that these assets exist in the first place. One side of this issue is the anonymous accounts (ref. Q.18 above), another is the rights of the administrator vs. custodians that hold control of the assets, and the third is the mass of potential counterparties that any holder of rights need to sue to enforce the claim in a distributed ledger. It should be considered how these issues can be accounted for in a set of private law principles. Granting the ledger "entity status" as proposed in Q.18 and our research may at least provide a step towards this solution.

133. Additionally, a representative from Switzerland has noted that:

A new Principle 20(1) should provide that "In case of the insolvency of a custodian, its client shall have protection described in Principle 14(3), if a custody agreement in the sense of Principle 12(3)(a) to (c) was concluded, even with regard to its assets that the custodian in violation of the agreement did not hold for the account of the client."

It would lead to inadequate results if clients lose their proprietary claim only because a custodian violates its duties. It is a matter of weighing up the expectations of clients and of the custodians' other creditors against each other. If statutory provisions or a generally known industry practice prescribe operational segregation of clients' and the custodians assets, clients should be able to rely in good faith on a preferred position. Conversely, other (ordinary) creditors should not expect their own claims to be satisfied with client assets. Accordingly, ordinary creditors should not be allowed to benefit from a violation of the custodian's segregation duties.

Finally, a new Principle 20(5) should provide for a solution for cases of shortfall. "(a) If the digital assets excluded from the insolvent custodian's estate are not sufficient to satisfy the protected clients in full, digital assets of the same kind held by the custodian for its own account shall also be excluded insofar as necessary. This shall apply even where such digital assets have been held separately from the clients' digital assets. (b) If the protected clients are still not fully satisfied, they shall bear the shortfall in proportion to the number of digital assets of the missing kind owed to them respectively. They shall have a corresponding claim for compensation against the custodian."

The proposal is inspired by Art. 19 of the Swiss Intermediated Securities Act, which serves nowadays for insolvency proceedings against all kinds of financial intermediaries. (<https://www.fedlex.admin.ch/eli/cc/2009/450/en#19>.)

134. In this regard, the DC has noted that the comment from the representative of Luxembourg seems to be raising issues of identifying/tracing digital assets in insolvency, which may be outside the scope of this project. UNCITRAL is currently considering a project on asset tracing.

135. The solutions proposed by the Swiss comment raise a question how far the WG is able to go in these Principles while remaining consistent with the existing international standards. There is no similar provision in Article 26 of the Geneva Securities Convention. These principles would not preclude any other protection, whether of private law or regulatory. This may be a matter of commentary to state that other protections could be made available.

