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

EN

Digital Assets and Private Law Working Group

Seventh session (hybrid)
Rome, 19-21 December 2022

UNIDROIT 2022
Study LXXXII – W.G.7 – Doc. 2
English only
December 2022

MASTER COPY OF THE DRAFT PRINCIPLES AND COMMENTS

TABLE OF CONTENTS

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 in paragraph 17). Without predictable results, the transactions will have inherent inefficiencies and there will be greater costs and 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.

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. The increased predictability should reduce the costs of these transactions, both in direct transaction costs and pricing. **See also Principle 5**

II. NEUTRALITY AND THE RELATIONSHIP OF PRINCIPLES TO NATIONAL LAW

5. These Principles take a practical and functional approach. This has several important effects. 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 done only to clarify the application of the Principles, and is not meant to favour that type of asset or 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 Principle 1. Scope.. On the definition of a Digital Asset, see Principle 2(2).

6. Second, these Principles are jurisdiction neutral. Therefore, these Principles have not been drafted using the terminology of a specific jurisdiction or legal system, 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 all jurisdictions, including 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. In substance the same result is reached. 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) and legal system. Traditionally, common and civil law jurisdictions use different strategies to address new

phenomena and to implement supra-national law, and these Principles do not prescribe a specific strategy. One jurisdiction, for instance, may elect to adopt a specific statute that is consistent with, or implements these Principles as a whole. Alternatively, another jurisdiction may elect to implement these Principles into existing law and amend it 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 one or more of 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 in such a way that their scope is more limited than that defined in these Principles. For instance, if a certain jurisdiction considers 'commercial law' to apply to merchants only and not to consumers, these Principles should not be implemented only into that jurisdiction's commercial law, because the scope of these Principles does not exclude consumers. Vice versa, these Principles should not be implemented only into a jurisdiction's consumer law, 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.

10. 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 unaffected 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, many of the legal consequences of third party effectiveness of a transfer of digital assets and some of 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.

III. SCOPE OF PRINCIPLES

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).**

12. In some cases a digital asset covered by the Principles will state that it is 'linked' to another asset". 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).**

13. The Principles extend to a Central Bank Digital Currency if it is in the form of a digital asset capable of being subject to control, namely, a digital asset that is within the the scope of the Principles.

IV. CORE CONCEPTS

14. Proprietary aspects. These Principles treat digital assets as being susceptible to being the subject of proprietary rights, without addressing whether they are considered 'property' under the other law of a State. **See Principle 1: Scope and Principle 3(1): General Principles.**

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 in this regard. **See Principle 5: Private International Law**.

16. Control. As discussed above in connection with the description of which digital assets are covered by 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. These Principles cover that set of transactions most important in commerce – transfers and secured transactions. 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 who has control of a digital asset will have priority over other secured creditors with a security right in the same digital asset who do not have control. These rights will benefit subsequent transferees under a 'shelter' rule. **See Principles 8 - 10** and Principles 14 - 17 (Section V: Secured Transactions).

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 11-13 (Section IV: Custody**).

V. TRANSITION RULES

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.

SECTION I: SCOPE AND DEFINITIONS

Principle 1: Scope

These Principles deal with the private law relating to 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). 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 (including, for purposes of these Principles and to simplify references, the creation of security rights) 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 required by public authorities.

2. Moreover, these Principles intend to address only 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 unaffected 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, some of 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.)

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 all technological and legal systems. 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.[2] On the technological, jurisdiction and organisational neutrality of these Principles, see the discussion in Part II of the Introduction above.

---

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. 4.

Principle 2: Definitions

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

1. 'Electronic records' comprise a class of which 'digital assets' (as defined in Principle 2(2)) form a subset. As defined, an 'electronic record' consists of information stored in an electronic or 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 using magnetic fields, and DVDs using 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.[3] Were it not for this provenance of the definition it might seem 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. Therefore, the definition of the term has been chosen that already has been generally accepted.

(2) '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 control (subject to qualifications in the definition).

4. Consider a simplified example: Three sets of information compose an electronic record. One set is ' Info Alpha' and a second set is 'key information' that, pursuant to public-key cryptography, renders these two sets 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.) These two sets of information compose the digital asset 'Digital Asset Alpha'. The third set of information is 'Info Beta'. Although Info Beta is associated with and included in the same electronic record as Digital Asset Alpha, a transfer of control of Digital Asset Alpha so that it becomes subject to control through the different key information of the transferee would not transfer control of Info Beta. Indeed, Info Beta is not (it is assumed) capable of being subject to control. This example is not unrealistic. For example, an interest in bitcoin is composed of an unspent transaction output (UTXO). The UTXO might be associated with information, such as information included in a header, that is a part of

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

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.

5. Continuing with the example of Digital Asset Alpha described in paragraph 4, pursuant to Principle 9 an innocent acquirer (X) of the Digital Asset Alpha would acquire it free of conflicting proprietary claims. But this would not mean that the X acquires Info Alpha (e.g., that the X 'owns' Info Alpha, even if that such information could be 'owned' under the applicable law). Instead, X acquires the Info Alpha only insofar as it is associated with the key information as a part of Digital Asset Alpha. Info Alpha exists not only as a component of Digital Asset Alpha but also independently and separate and apart from Digital Asset Alpha. Info Alpha is the same—'Info Alpha' is 'Info Alpha'—however or wherever that information might be stored, existing, or perceived. Digital Asset Alpha is distinct, however, because it is composed not only of the Info Alpha *but also of the key information*.

6. Info 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 the Principles law (see Principle 2(3), defining 'Principles law') the information would remain subject to any applicable laws other than the Principles law. If Info Alpha 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 Digital Asset Alpha. See Illustration 2. *infra*. On the other hand, it is possible that inclusion of Info Alpha in Digital Asset Alpha, or the use, transfer, or acquisition of Digital Asset Alpha, could violate, or infringe upon. rights under such laws. Even if Info 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 Digital Asset Alpha would not be affected by the Principles law.

7. The information such as Info Alpha included in a digital asset also must be distinguished from associated information such as Info Beta or any other asset in any way linked or associated with the digital asset. Principle 4 addresses such linked assets, for example gold or securities linked to a digital asset, as discussed in Illustrations 1 and 2 to Principle 4.

8. The following Illustrations to Principle 1 (Scope), Principle 2(1) (definition of 'electronic record'), and Principle 2(2) (definition of 'digital asset') 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), Principle 2(1) (definition of 'electronic record'), and Principle 2(2) (definition of 'digital asset')

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

9. In a public blockchain no one person controls the underlying protocol (software)— i.e., 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 itself would not be capable of being subject to 'control' as defined in Principle 6). However, an individual user does have control over a private key, which allows the individual user to obtain 'control' (as so defined) over a digital asset within the protocol (i.e., over a UTXO (unspent transaction output) in the case of bitcoin).

10. Although other public blockchains may differ from 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. A protocol within which a digital asset exists is not itself a digital asset within the scope of these Principles. An asset controlled by a private key however is a digital asset within the scope.

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

Illustration 2: If a digital asset contains information that is a valuable dataset/database (e.g., a 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.

12. 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.

13. 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 the Principles law and other law relating to digital 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. 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 asset is not a part of the digital asset.

Illustration 3: A social media page with password for access is not a digital asset.

14. Generalisations about social media/social networking platforms are difficult. But 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. Consequently they do not constitute or involve digital assets within the scope of these Principles.

Illustration 4: Although an Excel or Word file with password protection could be a digital asset, the Principles law may have no material impact or utility for such assets.

15. 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, 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 characterised 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) 'Principles law' means any part of State's law which falls within the scope of the Principles.

(4) 'Other law' means a State's law to the extent it is not Principles law.

Commentary

16. 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 rights in digital assets. Under this definition (3), all the rules provided by the Principles qualify as '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 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, (Introduction, Part II. Neutrality and the Relationship of Principles to National Law).

17. 'Principles 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.

18. Pursuant to its principles of functionality and neutrality, these Principles do not prescribe a specific classification of digital assets. However, these Principles do require that digital assets can be the subject of proprietary rights. (see Principle 3(1)). This may mean, in certain jurisdictions, that digital assets must be classified as 'property', 'good', 'thing', or similar concept, but this would depend on the applicable law in question and is left for the specific States to decide. If a State's law includes a classification of different categories of assets which can be subject to proprietary rights, and these different categories have different consequences, it is recommended that the State's law should specify which category or categories of assets digital assets are. This is so that digital assets can be subject to proprietary rights. This could mean the introduction of a new category of asset, but again, this is left for the specific States to decide.

19. More generally, if, in a specific State, it is unclear, which (if any) of its existing rules or standards of general application apply to digital assets, it is recommended this is clarified. This is specifically relevant where it concerns the acquisition and disposition of proprietary rights in digital assets. This may also mean, for instance, that States should 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. See also the commentary to Principle 3(1) below.

20. Within a State's law, all law that is not 'Principles law' as defined here, is referred to as 'other law' in these Principles. 'Principles law' AND 'other law' as defined here together form 'the law'.

(5) 'Transfer' of a digital asset means the change of a proprietary right in the digital asset from one person to another person.

(a) The term 'transfer' includes the acquisition of a proprietary right in a resulting digital asset.

(b) 'Transferor' means a person that initiates a transfer and 'transferee' means a person to which a proprietary right is transferred.

(c) The term 'transfer' includes the grant of a security right in favour of a secured creditor, and a 'transferee' includes a secured creditor.

(6) 'Resulting digital asset' has the meaning specified in Principle 6(2).

(7) [Unless the context otherwise requires, words] [Words] in the singular number include the plural and those in the plural include the singular.

Commentary

21. A transfer, as defined in Principle 2(5), includes not only the transfer of a digital asset from one person to another person but a transfer that results in the acquisition of a resulting digital asset that is not the same digital asset that was transferred by the transferor. An example of such a resulting 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.

22. In these Principles, the term 'transfer' is also used to denote the grant of a security right in favour of a secured creditor, and a 'transferee' includes a secured creditor. This use of the term transfer is for definitional purposes only, and does not mean that pursuant to these Principles, a grant of a security right must be identified with a transfer of ownership or of any other proprietary right under the applicable law. See, e.g., Hague Securities Convention, art 1(1)(h) (defining 'disposition' as 'any transfer of title whether outright or by way of security and any grant of a security interest, whether possessory or non-possessory').

23. A transfer as defined here, i.e. a change of a proprietary right in a digital asset, must be distinguished from a change of control of a digital asset (as defined in Principle 6). A change of control may or may not be associated with a transfer of proprietary rights. A custodian (as defined in Principle 11), for instance, may obtain control of a digital asset for a client, but will typically not acquire 'ownership' (as defined under the applicable national law) of that digital asset. Vice versa, a transfer of proprietary rights may or may not be accompanied by a change of control. A State's law, for instance, may provide that under certain circumstances a proprietary right (such as ownership) in a digital asset may pass to another person, whilst control stays with the transferor.

24. These Principles do not prescribe the conditions for a proprietary right in a digital asset to be validly transferred to another person. Although Principle 3(1) does require that digital assets must be susceptible to proprietary rights, and Principle 8 that a transferee must have obtained control to qualify as an innocent acquirer, these Principles do not prescribe the requirements for a valid transfer of a digital asset. For instance, they do not prescribe whether a change of control

suffices or is required for a change of a proprietary right to be valid. This is left to other law. See also below, Principles 3(1) and 3(3).

25. The term 'transferor' is defined as 'a person that initiates a transfer' because the person may have the power to transfer greater rights than the person has. Indeed, a person in control of a digital asset may have no rights at all but has the power to transfer rights to an innocent acquirer. See Principle 8(d) and Commentary paragraph 2.

26. Principle 2 (7) contains a general rule of interpretation that applies to the whole of the Principles. For example, if 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.

Principle 3: General principles

(1) A digital asset 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 premise. 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,[4] these Principles advise States to increase legal certainty on this issue and make explicit that digital assets can be the subject of proprietary rights. What is meant by 'proprietary rights' is discussed in paragraph 4 below.

2. Whether digital assets can be the subject of proprietary rights (a legal consequence) must be distinguished from the classification of digital assets. As explained in the commentary to Principle 2(3), these Principles do not prescribe a specific classification of digital assets. That digital assets must be susceptible to proprietary rights as this Principle 3(1) requires, may mean, in certain jurisdictions, that digital assets must be classified as 'property', 'good', 'thing', or similar concept, but this would depend on the applicable law in question and is left for the specific States to decide. If a State's law includes a classification of different categories of assets which can be subject to proprietary rights, and these different categories have different consequences, it is recommended that the State's law should specify which category or categories of assets digital assets are. This is so that digital assets can be subject to proprietary rights. This could mean the introduction of a new category of asset, but again, this is left for the specific States to decide.

3. Principle 3(1) also leaves to other law (as defined in Principle 2(4)) issues such as whether a person has a proprietary right in a digital asset and whether a proprietary right in a digital asset has been validly transferred to another person. Whilst this Principle 3(1) does require that digital assets must be susceptible to proprietary rights, it does not prescribe, for instance, the specific requirements for a valid right of ownership in a digital asset or for a valid transfer of the same. These issues are left to other law. See also Principle 3(3) and its commentary.

4. '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, i.e. 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.

(2) Principles law takes precedence over other law to the extent that they conflict.

5. These Principles provide specific rules for the holding, transfer and use of digital assets, 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

[4] [sources to be added]

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)).

6. As already stated above, these Principles take no position as to whether its rules should be included in a special law on digital assets enacted by a State, incorporated into more general laws of a State, already follow from the general law of a State, or are addressed by a combination of these approaches. However, Principles law (as defined) takes precedence over other law (as defined). See also Principle 2, commentary especially paragraph 19.This may be achieved in a State as a result of generally applicable rules that grant precedence to specific laws over general laws, or to later laws over earlier laws. A State may need to specify the laws and sections/articles in other laws that are repealed or superseded.

(3) Except as displaced by these Principles, other law applies to all issues, including

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

(b) whether a proprietary right in a digital asset has been validly transferred to another person;

(c) whether 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 a digital asset; and

(g) the requirements for, and legal consequences of, third party effectiveness of a security right in a digital asset.

Commentary

7. Principle 3(3) makes it explicit that other law, i.e. all law within a given State that is not 'Principles law' as defined in Principle 2(3), continues to apply to digital assets. For this purpose, Principle 3(3) lists several examples of issues of property law, but also of contract law, that may continue to be addressed 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 cover only 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 unaffected by them. Finally, there are several issues of property and contract law that these Principles do not cover, and Principle 3(3) lists important examples of 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.

8. The examples in Principle 3(3) of issues that continue to be addressed by other law, can be categorised 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 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 a certain digital asset, is, as a matter of principle, not regulated by these Principles.

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, Principles 3(3)(b) and (c) make it clear that the requirements for a (valid) transfer and creation of a security right continue to be, as a matter of principle, a matter of other law. See Principle 2(5) for the definition of transfer as used in these Principles. However, these Principles do provide some specific rules regarding the transfer of, and third-party effectiveness (perfection) of a security right in, a digital asset. For example, Principle 15(1) provides that control (as defined in Principle 6(1)) must be an available method of making a security interest in a digital asset effective against third parties, but other law may provide for other means of ensuring effectiveness. Moreover, Principle 8 provides that an innocent acquirer takes free from conflicting proprietary rights and Principle 10 provides similar protection to a client for whom a custodian maintains a digital asset. Whenever it is unclear whether existing rules or standards of general application apply to digital assets, and whenever Principles law derogates from other law, it is recommended that State law makes this explicit.

10. Principles 3(3)(d) and (e) make explicit that the relationships between a transferor and transferee, and between a grantor 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, dealt with 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 a digital asset and the transferee, and between a grantor of a security right in a digital asset and the secured creditor, are left to be dealt with by other law, whatever the qualification of the relationships between those parties. See Principle 2(5) for the definition of transfer as used in these Principles.

11. As explained above, Principles 3(3)(d) and (e) concern the (contractual) relationships between a transferor and transferee, and between a grantor 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 security right, 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'. 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.

Principle 4: Linked assets

These Principles apply to a digital asset linked to another asset, whether the other asset is tangible or intangible. Other law applies to determine the existence of, requirements for, and legal effect of any link between the digital asset and the other asset.

Commentary

1. As provided in Principle 4, a digital asset may state that it is linked to another asset or assets. Principles law takes a neutral stance as to whether this link is sufficiently established and what, if any, the legal effect of the link may be. These matters are instead left to the other law of the State, including its regulatory law, to determine. Consequently, the link between the digital asset and the other asset may operate in a variety of different ways.

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 be 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. Consistently with the primacy of other law under Principle 4, the operation of linked assets 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 other law of the State (including its regulatory law) may define minimum standards of certainty for recognising the link. A link which failed to satisfy 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 factual 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. It 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. Consistently with the primacy of other law under this Principle, the parties who issue or transact with the digital asset cannot confer any greater legal effect on the link than the other law of the State would allow. In this way, transactions with linked digital assets do not necessarily have the same legal effect as transactions with conventional assets, such as 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 an existing rule of

other law 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 the 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 may be required to change the parties' rights to the other asset. Thus the legal effect of holding and transferring linked assets depends on a combination of these Principles and any rules of other law relevant to the other asset.

9. As part of this process, 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 8 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. See illustration 7 below.

10. As illustrations of the different legal effects of a link between the digital asset and the other asset, [7] examples follow:

11. ***Illustration 1***: The rules of other law already in force may apply to the parties' transaction with the digital asset and determine the legal effect on the other asset linked to it.

12. For example, a system may be established for trading quantities of tokenised gold. An investor may hold a digital token which evidences a proprietary right in a fractional share of specifically identified gold. Whether a sale and transfer of the token passes the seller's proprietary right in the gold depends on the rules of other 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 directly 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 to 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.

13. ***Illustrations 2 and 3***: A State may choose to enact special legislation to make the link between the token and the other asset legally effective.

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 claim against the debt issuer. The terms of issue purport to give the investor a right to payment by the debt issuer. When the token is transferred on the ledger, the transferee acquires the right against the debt issuer. The company which issued the debt security gets an effective 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 State's existing other law of contract, assignment, novation or securities transfer.

15. As a further example, a State may enact special legislation that creates digital equivalents to paper negotiable instruments or documents of title to goods. The legislation may provide that a

transfer of control of the digital asset has the same legal effect as the delivery of possession of the paper document to which it is equivalent. Depending on the State's existing other law, the effect may be that the transferee of the digital asset would acquire the right to claim on a monetary debt or a title to the goods linked to the digital asset. The special legislation would define minimum criteria that the digital asset would need to satisfy if it were to serve as a legal equivalent to the paper documents in the existing other law of the State.

16. ***Illustration 4***: The precise legal effect of any link between the digital asset and 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 other law. Thus, the terms of a White Paper accompanying the issue of a 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 to the other asset.

17. 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. 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.

18. 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. 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 not also have a proprietary right in the other assets held in the reserve. It would be for the insolvency rules of the other law to determine how, if at all, this right might take priority over any other claims enforceable against the issuer.

19. ***Illustration 5***: Digital assets may be used to create transferable portions of value derived from other assets which exist off the blockchain. Even when the link between the digital assets and the other assets is clear, the precise effect of the holders' rights will be determined by the other law of the state. The parties' intention to link the assets cannot override the other law that applies to those assets.

20. 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 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 to update a company register; or update a register of real estate.

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

22. [States could, if they wish, require, as a matter of regulation, disclosure of information as to any purported link between the digital asset and the other asset, and, if desired, could specify the form that that disclosure must take.]

23. **Illustration 6:** 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.

24. 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 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 return, the holder's wrapped digital asset would be "burned". The effect of this 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, 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 "burned" at that point.

25. **Illustration 7:** 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.

26. 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 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 law of the state to determine whether the innocent buyer would also acquire a proprietary right in the 'linked' share of the gold and also take it free of the original investor's claims.

27. The other law of a state may provide similar consequences for a linked asset subject to a security right, as in Principle 16. A security right may be taken in a digital token that purports to evidence a proprietary right in a fractional share of gold. Whether the security right extends to the gold is a matter of other law. Developing the in Illustration 3 above, the other law may, for instance, treat the digital token evidencing a proprietary right to gold as a document of title, in which case a security right in the token would extend to the gold. Any such system would have to consider carefully how to address rights in the linked asset so that all rights "reside" in the token.

28. If other law provides similar consequences for the good faith acquisition of the digital asset as the other asset, then the innocent acquirer of a digital asset may take both assets free of the security right. But consistently with the primacy of other law, the rights of any innocent acquirer in relation to the other asset may be determined by legal rules which are different from the principles law relevant to the digital asset itself. States may therefore need to enact special legislation to ensure that the rights of a third party acquirer in relation to the digital asset and the linked asset remain in line with each other.

SECTION II: PRIVATE INTERNATIONAL LAW

Principle 5: Conflict of laws [5]

(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:

OPTION A:

(i) [the forum state should specify here the relevant aspects or provisions of its law which govern proprietary issues in respect of a digital asset];

(ii) to the extent not addressed by clause (i), [the forum state should specify here either that 'these Principles' govern proprietary issues in respect of a digital asset or should specify the relevant Principles or aspects of these Principles which govern proprietary issues in respect of a digital asset]; and

(iii) to the extent not addressed by clauses (i) or (ii), the law applicable by virtue of the rules of private international law of the forum.

OPTION B:

(i) [the forum state should specify here either that 'these Principles' govern proprietary issues in respect of a digital asset or should specify the relevant Principles or aspects of these Principles which govern proprietary issues in respect of a digital asset]; and

(ii) to the extent not addressed by clause (i), 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 issues in respect of digital assets, and in particular their acquisition and disposition, are always a matter of law.

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.

---

[5] [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.]

(c) By transferring, acquiring, or otherwise dealing with a digital asset a person [consents] [is deemed to consent] to the law applicable under paragraph (1)(a) and (b).

(d) The law applicable under paragraph (1) applies to all digital assets of the same description from the time that a digital asset is first issued or created.

(e) If a digital asset or the system or platform on which the digital asset is recorded expressly specifies the applicable law effective from a time after the time that the digital asset is first issued or created, rights and interests in the digital asset that are established before the express specification becomes effective are not affected by the specification.

(3) Notwithstanding the opening of an insolvency proceeding and subject to paragraph (4), the law applicable in accordance with 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.

(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 an asset that is part of the insolvency estate or under the supervision of the insolvency representative.

(5) This Principle does not apply to the extent that proprietary issues are addressed by a system for registration of security rights [or] [additional issues, if any, to be excepted from this Principle which are specified by the forum state].

(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

Commentary

1. [Principle 5 addresses the applicable law for proprietary issues in general and is not limited to those issues that are covered by the Principles. The law of the forum determines what would qualify as 'proprietary issues'. This broad scope of Principle 5 is to prevent the issues covered by these Principles, which are limited in scope, being governed by laws different than those governing proprietary issues that are closely connected with the issues covered by these Principles, but fall outside its scope. See, e.g., the issues listed in Principle 3(3).]

2. [Principle 5 addresses the applicable law only 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.]

3. 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 because digital assets are intangibles that have no physical situs. 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.

4. Paragraph (1) provides a 'waterfall' of factors for the determination of the applicable law. Under paragraph (1)(a), 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) treats every person dealing with a digital asset as consenting to the choice of law rules in paragraph (1). Persons who could be affected by a determination of a proprietary issue would be treated as having consented. This reliance on party autonomy is consistent with Article 3 of the Hague Conference Principles on Choice of Law in International Commercial Contracts ('Hague Conference Principles'). 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.

5. 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), paragraph 1(c) provides a state with a considerable degree of freedom to choose the appropriate rules for a forum sitting in that state. An overarching consideration is the fact that in many cases the digital asset may have no significant connection with any state. It is not feasible to specify in paragraph 1(c) a definitive, "one size fits all" approach to be applied by the forum to proprietary questions in respect of a digital asset. Paragraph (1)(c) provides for two Options (A and B): each includes the provision of some or all of the Principles to such questions. 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 (see Article 3 of the Hague Conference Principles that 'allows the parties to choose not only the law of a State but also "rules of law", emanating from non-State sources.')

6. Within each option in Paragraph (1)(c), there is a 'waterfall' set out in sub-paragraphs. The wording inside the square brackets found within the various sub-paragraphs explains what content the forum state should include within that square bracket, in order to specify what legal provisions apply in respect of proprietary issues in relation to a digital asset.

7. Option A recognises that a state may determine that it is appropriate for the forum sitting in that state to apply some aspects of its own domestic laws. This might be the case, for example, if the state has adopted laws that deal specifically with proprietary issues relating to digital assets. The aspects of domestic laws form the first part of the waterfall (sub-paragraph (1)(c)(i) of Option A). Within this sub-paragraph, the state should specify those aspects of its domestic laws that should be applied, as a matter of Private International Law in respect of proprietary issues in relation to a digital asset. The second part of the waterfall, in relation to matters not addressed by paragraph (1)(c)(i), is comprised of either the (entire) Principles, or some Principles or some aspects of the Principles. Which of these is the case should be specified by the forum state within sub-paragraph 1(c)(ii). The third part of the waterfall, which applies to the extent not addressed by other clauses, requires the forum to apply the law otherwise applicable under its private international law rules.

8. Option B consists of the second and third parts of the waterfall set out in Option A. It therefore is suitable for a state which determines that proprietary issues relating to digital assets should be determined only by the Principles or some portions thereof, without any reference to substantive domestic laws. This might be the case, for example, if the state has not adopted laws that deal specifically with proprietary issues relating to digital assets.

9. By making reference to these Principles, 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. Principle 5 leaves considerable flexibility for a state to craft choice-of-law rules that conform to its policy judgments and are compatible with its domestic laws.

10. 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, and (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.

11. 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.

12. 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.

13. Paragraph (5) recognises that the approach taken in paragraph (1) would be inappropriate for the law governing a registration system for security rights, which must be based on objective indicia (such as the location of the grantor) that could be determined by a third-party searcher of the registry. A forum state also may provide additional exceptions.

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 prevent others from obtaining substantially all of the benefit from the digital asset;

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

(iii) the exclusive ability to transfer the abilities in (i), (ii) and (iii) to another person (a "change of control").

(b) the digital asset or the relevant protocols or system 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 "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 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

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. However, 'possession' in this context is a purely factual matter and not a legal concept. Moreover, because a digital asset is intangible, this functional equivalence to possession involves only the dominion and power over a digital asset but does not involve the physical situs dimension applicable to 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. Although control assumes a role that is, as a purely factual matter, a functional equivalent to that of 'possession', control as used in these Principles must not be understood to be identical to 'possession' as a legal concept used in certain jurisdictions. In those jurisdictions, possession is a legal concept and a possessor may 'hold' possession of an asset through another person. However, under these Principles control is a factual matter and a person cannot control a Digital Asset unless the criteria of this Principle 6 are met. On the custody of Digital Assets, see also below, Principle 11.

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 a digital asset or an interest therein, i.e., a transfer of proprietary rights. See Principle 2(5) (defining "transfer"). A custodian (as defined in Principle 11), for instance, may obtain control of a digital asset for a client, but will typically not in that context acquire 'ownership' (as defined by the applicable national law) of that digital asset. Vice-versa, a transfer of proprietary rights may or may not be accompanied by a change of control. A State's law, for instance, may provide that under certain circumstances 'ownership' (as defined by the applicable national law) in a digital asset may pass to another person, whilst control stays with the transferor. This explanation reflects the understanding of 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'. Two illustrations of change of control are given in paragraph 13 and 14 below.

5. Control by a person of a digital asset as agent (for example, an employee may have control for their employer), is treated in these Principles as control by the principal, as an implementation of the law of agency. The concept of control also is relevant in the context of the custody of digital assets. As set out in Principle 11, under a custody agreement a service provider is obliged to maintain digital assets for its clients, either by controlling the digital assets itself or by entering into a custody agreement with a sub-custodian whereby the sub-custodian controls the digital assets for the service provider. The private law (as well as a regulatory framework) may require a custodian to maintain 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.

'Ability' of a person with control

6. 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 8-12 below.

7. 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. 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) 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. This underscores the distinction between a change in control and a transfer of proprietary rights.

9. 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 has 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 is the improper taking of physical possession of a tangible object from a person in physical possession of the tangible object). 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.

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 may result in changes, including a change in control, which constitute exceptions to the exclusivity of a control person's abilities. Paragraph (3)(b) recognises 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.*

11. Paragraph (1)(a)(iii) of this Principle does not require that the specified ability 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 would be of no (legal) consequence that a control person has elected to permit another person (or persons) to obtain the 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 would be of little or no consequence. In any event, a control person need not prove a negative fact, as provided in Principle 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.

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).

Illustrations 2 and 3 : change of control

13. **Illustration 2: Transfer of control via PKI**: A public, permissionless, distributed network (Alpha) supports a virtual machine (Alpha-VM) that enables the creation and use of electronic records

(Beta) in its database (Alpha-DB). Alpha implements a public-key cryptography system, whereby every Beta is associated with a public key and can be used only by a person who sends the appropriate instructions to the Alpha-VM validated by the corresponding private key. Alpha and the Alpha-VM support two uses for Betas. First, a person can actuate a Beta to record a small image file into the Alpha-DB permanently; each Beta can be actuated only once. Second, a person can change the public key with which a Beta is associated; after a Beta has been associated with a new public key, its corresponding private key is required to use that Beta.

14. A Beta is a digital asset, as it satisfies all the requirements of Principles 2 and 6. Person A transfers control of a Beta to Person B by disassociating the Beta from a public key for which only Person A knows the private key, and associating it with a public key for which only Person B knows the private key.

15. **Illustration 3: Transfer of control via OTP-Device:** A private, permissioned, distributed network (Gamma) supports a virtual machine (Gamma-VM) that enables the creation and maintenance of electronic records (Delta) in its database (Delta-DB). Deltas are records capable of storing only unformatted text. Gamma implements a form of hardware security, whereby each Delta is paired with a hand-held device that randomly generates one-time passwords (OTP-Device). To read, edit and delete text stored in a Delta, a person requires a one-time password generated by the OTP-Device paired with the Delta in question.

16. A Delta is a digital asset, as it satisfies all the requirements of Principles 2 and 6. Person A transfers control of a Delta to Person B by physically handing to them the OTP-Device paired with that Delta.

Principle 7: Identification of a person in control of a 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 (1)(b) is satisfied in respect of the abilities specified in Principle 6 (1)(a);

(b) if that person demonstrates that it has the abilities specified in Principle 6(a)(i) and (ii), those abilities are presumed to be exclusive.

(2) The identification mentioned in Principle 6 (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 (1) of this 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. 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. The presumption can be overcome by sufficient proof under the State's procedural rules.

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.

Principle 8: Innocent acquisition rule

(1) (a) An innocent acquirer takes a digital asset free of conflicting proprietary rights ('proprietary claims').

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

(c) In order to qualify as an innocent acquirer, a transferee must obtain control of a digital asset.

(d) An innocent acquirer can acquire a proprietary right in a digital asset even if control of that digital asset is changed by a transferor 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) In addition to the requirement in sub-paragraph (1)(c), 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.

(4) If these Principles are applied pursuant to Principle 5(1)(c)(i), in addition to the requirement in sub-paragraph (1)(c), the following requirements for a transferee to be an innocent acquirer apply with respect to digital assets of the relevant type [This chapeau to be revised to conform with changes made/to be made to Principle 5(1)(c)]:

(a) A transferee of a digital asset is an innocent acquirer of a digital asset unless, at the time the transferee takes control of the digital asset, the transferee actually knows or ought to know that another person has an interest in the digital asset and that the acquisition violates the rights of that other person in relation to its interest.

(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 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.

Commentary

1. The rights conferred on innocent acquirers in accordance with subparagraphs (a) and (b) of paragraph (1) 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 (1) 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 innocent acquirer. See also the discussion in Principle 6, Explanation and commentary, paragraphs 3 and 4.

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 for other types of assets. A State might wish to adopt slightly different innocent acquisition rules for different types of digital assets.

4. Paragraph (4) provides a default set of requirements for a transferee to be an innocent acquirer 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 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 displaced by these Principles, other law continues to govern issues relating to a digital asset.

Principle 9: Rights of transferees

(1) Subject to Principle 8, a person can transfer only the proprietary rights that a person has in a digital asset, if any, and no greater proprietary rights.

(2) A transferee of proprietary rights in a digital asset acquires all of the proprietary rights that its transferor had or had the power to transfer, except that the transferee acquires rights only to the extent of the rights that were transferred.

Commentary

1. Principle 9(1) states the familiar rule of nemo dat quod non habet—no one can give what one does not have. Principle 9(1) is subject to the innocent acquisition rule in Principle 8, which operates as an exception to the consequences of the application of the nemo dat rule. The effect of Principle 8 is not that the transferor transfers more proprietary rights than it itself has, but that an innocent acquirer takes free of conflicting proprietary rights, and that no rights based on a proprietary claim can be asserted against an innocent acquirer.

2. Principle 9(2) states the shelter principle: a transferee acquires all the rights of the transferor that were transferred or that the transferor had the power to transfer. Principle 9(2) makes an exception for the situation in which a transferor transfers less than all of its rights in the digital asset, in which case the transferee acquires only the rights that were transferred.

3. Pursuant to Principle 9(2), a transferee from a person that was an innocent acquirer of proprietary rights in a digital asset and any subsequent transferee acquires the rights of the innocent acquirer, that is, rights free from conflicting proprietary rights and the successful assertion of conflicting proprietary claims. This is the case even though the transferee at the time of the transfer would not itself meet the applicable requirements as an innocent acquirer (e.g., if it had the knowledge specified in Principle 8(4)(a), if applicable, with respect to the digital asset).

Principle 10: Innocent client rule

(1) Subject to paragraph (2), where a custodian maintains a digital asset pursuant to a custody agreement as defined in Principle 11(3), no rights based on a proprietary claim to that asset may be successfully asserted against the client.

(2) Paragraph (1) does not apply if the client, at the time from which the custodian maintains the digital asset for that client., actually knows or ought to know that another person has an interest in the digital asset and that the acquisition violates the rights of that other person in relation to its interest.

(3) In this Principle,

(a) "custodian" includes a sub-custodian, in which case "client" refers to the custodian who is the client of the sub-custodian;

(b) the term "digital asset" includes a resulting digital asset.

(4) If digital assets are maintained by a custodian for two or more clients in an undivided pool, Principle 10(1) and 10(2) applies to each client for whom the digital assets are maintained.

Commentary

1. This Principle addresses the situation where a custodian or sub-custodian obtains control of a digital asset and maintains that asset for a client or a group of clients, if the asset is maintained in a pooled account (the latter situation is addressed in paragraph 7 below). It provides that the client cannot be subject to a successful claim to that asset brought by a person whose rights are violated by the change of control to the custodian, unless the client knows or ought to have known of that violation of rights. It is, therefore, an adaptation of the innocent acquisition rule tailored for the circumstances of custody. The standard of 'innocence' is that set out in Principle 8(4)(a), although, in accordance with Principle 8(3), a State has flexibility to adapt this standard to be consistent with its own good faith purchase and taking free rules.

2. This principle applies at each level of custody, if there is more than one level. Thus, if a sub-custodian maintains an asset for a custodian (who then maintains that asset for a client, see Principle 11(2)), Principle 10(1) applies to that custodian as client (vis a vis the sub-custodian). Principle 10(1) also then applies to the client of the custodian because the custodian maintains that asset for that client.

3. There are a number of ways in which a custodian could come to control a digital asset for a client. Depending on the factual situation and the manner in which the applicable law analyses that situation, the position of the client is governed either by Principle 8 (Innocent acquisition rule) or Principle 10. Some illustrations of possible situations are set out in the next paragraphs.

Illustration 1

4. If a custodian obtains control of a digital asset in the course of a transfer of that asset to it for its own account in a situation where the custodian was an innocent acquirer under Principle 8, and then, as part of a subsequent sale transaction, the custodian transfers the asset to a client and subsequently maintains that digital asset for its client, there would be no need for Principle 10 to apply. This is because, under Principle 9(2) no successful claims in respect of the asset could be made against the custodian, and therefore no successful claims could be made against the client for whom the custodian maintained that digital asset. Principle 9(2) provides that a transferee acquires all the proprietary rights that its transferor had.

Illustration 2

5. If a client instructed its custodian to obtain a [particular] digital asset on its behalf, in circumstances where the custodian acted purely as an agent or representative of the client, it is likely that the client would also qualify as an innocent acquirer under Principle 8 if the control by the custodian was treated as that of the client and the client otherwise satisfied the requirement for innocent acquirer status.

Illustration 3

6. If a custodian obtained control of a digital asset in circumstances other than those in Illustration 2 in order to maintain it for a client (or a number of clients in the case of a digital asset to be held in an undivided pool (see Principle 12(2)) Principle 10 would apply.

7. Principle 10 applies equally whether the digital asset(s) maintained for a client are maintained in a separate segregated account or in an undivided pool. As stated in Principle 10(4), where the digital assets are maintained in an undivided pool, Principle 10 applies to each client in the same way. Thus, unless a client knows or ought to know of another person's violated right to a digital asset which forms part of the pool, no claims can be asserted against that client in respect of that asset or any others in the pool. Principle 10 does not affect the position of the clients in the pool with respect to each other, which is that all clients share rateably and proportionately in the pool, including on the insolvency of the custodian (see Principle 13(3)).

SECTION IV: CUSTODY

Principle 11: Custody

(1) (a) "Custodian" means a person who provides services to a client pursuant to a custody agreement as defined in Principle 11(3);

(b) "Client" means a person to whom a custodian provides services pursuant to a custody agreement as defined in Principle 11(3);

(c) "Sub-custodian" means a person who provides services to a custodian pursuant to a custody agreement as defined in Principle 11(3) in the circumstances set out in Principle 12(4).

Commentary

1. The purpose of this Section is to set out principles relevant to custody of digital assets. Custody, broadly speaking, is where a person (usually a legal person, which may be a regulated entity), maintains a digital asset on behalf of and for the benefit of another, a client (which may be another custodian), in a manner that gives the client special protection against unauthorised dispositions of the asset and against the insolvency of the custodian who maintains the digital asset. It only applies when the person providing the custody services does so in the ordinary course of its 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, although the precise technique 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 may control a digital asset while another person (the client) may have 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 Principle states about custodians only applies to custody services and not to other services provided by those persons.

3. Whether the services provided by a business are custody services will depend on whether the agreement between the business and its client is a custody agreement. Principle 11(3) defines a custody agreement. Principle 11(1) defines the important parties in relation to custody. The person controlling the asset is either a 'custodian' (in which case it controls the assets for a 'client' who is not a custodian) or a "sub-custodian" (in which case it controls the asset for a client who is a custodian, and who has entered into a custody agreement with a client in relation to that asset.)

(2) a custodian maintains a digital asset for a client if

(i) that custodian controls the digital asset, or

(ii) a sub-custodian controls, or maintains through another sub-custodian, the digital asset for that custodian pursuant to a custody agreement as defined in Principle 11(3).

Commentary

3. The purpose of Principle 11(2) is to introduce the concept of 'maintaining' a digital asset, which is wider than the (factual) concept of 'control' as defined in the Control Principle. The word 'maintain' is defined as encompassing two situations in which a custodian 'maintains' a digital asset for a client. The first is where a custodian controls an asset within the meaning of the Control Principle. The second is where a custodian is the recipient of custody services, that is, where another custodian controls the asset for that custodian. Here, the person who controls the asset is a 'sub-custodian'. Where a sub-custodian is used, the sub-custodian and the custodian both 'maintain' the asset. There could also be more than one layer of custodians. For example, if there were three layers, the sub-custodian itself 'maintains' the asset for the custodian, because a third custodian controls the asset for that sub-custodian.

(3) Subject to sub-paragraph (4), 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 ordinary course of the service provider's business;

(b) the service provider is obliged to obtain (if this is not yet the case) and to maintain the digital asset for 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).

(4) An agreement to which sub-paragraphs (3)(a), (3)(b) and (3)(c) apply is not a custody agreement if it is clear from the agreement that the client does not have the protection set out in Principle 13(1).

Commentary

4. Principle 11(3) and Principle 11(4) provide a method to identify whether an agreement is a custody agreement or not. They perform two functions.

5. First, sub-paragraphs (a), (b) and (c) of Principle 11(3) serve as a definition of a custody agreement, and therefore of custody. Sub-paragraph (a) makes it clear that to be a custodian, a service provider must be acting in the ordinary course of its business. Sub-paragraph (b) sets out the core duty of a custodian, see also Principle 12(1). It covers three situations. The first is where the custodian, having entered into a custody agreement with the client, does not control the digital asset which is the subject matter of the agreement. For example, (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) if the custodian has exercised a (limited) right of use (see Principle 11(1)); or (3) if a custodian in is breach of its obligations and fails to control the digital asset that is the subject of the custody agreement. In all of these situations, the custodian is obliged to obtain the digital asset which is the subject of the agreement. If the digital asset is considered fungible, the obligation will be to obtain a digital asset of the type specified in the agreement, see Principle 2 commentary paragraph 26. The second is where the custodian does control the digital asset, in which case the custodian is obliged to continue to control that digital asset until otherwise instructed by the client or until the custodian exercises its right of use, if it has one (see Principle 12(1)(a) and (b)). The third is the situation where a custodian does not control the digital asset itself, but is the recipient of custody services, that is, where a sub-custodian controls the asset for that custodian. In the second and third situation the custodian 'maintains' the digital asset under the definition in Principle 11(2). Sub-paragraph (c) makes it clear that an agreement is not a custody agreement if the client has the exclusive ability to change the control of the digital asset. This situation is discussed in paragraphs 9 - 14 below. 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).

6. The second function is to address 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 (such an agreement is discussed in paragraph 15 below). This latter type of agreement can look similar to a custody agreement, as both are situations in which 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, under the latter type of agreement any assets controlled by the account provider form part of its assets for distribution to its creditors, and so 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 the risk is not present under a custody agreement (as long as the custodian fulfils its obligation to maintain the digital asset). For this reason, an agreement under which the client does not have control is presumed to be a custody agreement unless it is made clear in the agreement that assets held by the service provider form part of that party's assets available for distribution to its creditors. Principle 11(4) is designed to act as an incentive to service providers to make the nature of the agreement clear on its face.

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. (Of course, a state may wish to impose regulatory requirements on custodians, as well.) Various options for such regulatory protection are set out in paragraph 16 below.

Illustrations

8. There are a number of situations where a person controls a digital asset which are not custody and where any agreement with a service provider is not a custody agreement, as defined in Principle 11(3). The following paragraphs describe and illustrate examples of these situations.

9. **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. 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) 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 hardware or software is purely contractual and is governed by the terms of the agreement between them.

<u>Self-Custody and/or Non-Custodial Third-Party Wallet</u>

10. Self-custody is when 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: the chief difference is in the location where the private keys are held. In both cases, the client controls the digital asset.

<u>Software</u>

11. The term "self-custody" is often used to describe software provision of this type. It refers to the use of wallet software, which operates in an analogous way to the way coins and notes are kept in a physical wallet. In this example, XX is open source software, developed by a global community of developers and designers. It is compatible with a variety of hardware wallets. The user of XX creates a wallet password and Secret Recovery Phrase, which are stored, together with the private

keys, in an encrypted format on the mobile phone or computer on which the XX software is installed. Transactions conducted through wallets using XX software are broadcast on-chain.

Non-custodial wallet (software-as-a-service)

12. Y (a business) provides a non-custodial wallet for users. A user creates an account, and creates a password, which gives the user access to an encrypted file kept by Y on the blockchain containing a 'seed' (a Secret Private Key Recovery Phrase), the users' private keys and addresses of digital assets. The password is not stored by Y, and must be kept safe and confidential by the user herself. Y has no access to the user's private keys, seed or password. When a password or seed phrase is used correctly, the file containing private keys is decrypted locally on the user's computer or mobile phone, and the user can carry out transactions, which are conducted directly on-chain. Y stores the encrypted file in the cloud, while when the XX software is used (see above paragraph 11, the encrypted file is stored locally on the user's computer or mobile phone. Users of the software-as-a-service model, therefore, could find themselves in difficulty should Y ever decide to stop providing the wallet services.

13. **Where a business provides 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 safeguarding its private keys. Depending on the features, 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 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 Business model is therefore not a custody service as defined in this Principle, even though it is sometimes called "custody" by market participants. In contrast, where a business provides a custody service, its clients transfer their digital assets to addresses or private keys controlled by that business, or the business acquires digital assets which it controls on behalf of the client. An example of safeguarding of private keys is as follows:

14. The Z 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 Z hardware is not intermediated, as no third party intermediary has access to the keys held on the Nano wallet. When a user wants to transact with the keys held in a Z wallet, they use software similar to a mobile phone app store to access services provided by other providers to send, buy, or sell digital assets.

15. **An 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. 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.

16. 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.

17. Digital autonomous organisations (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.

18. **Illustrations of custody** There now follow a number of illustrations of situations in which the relationship between the service provider and the client is one of custody.

Custodial or Hosted Wallet

19. In a custodial or hosted wallet arrangement, users transfer digital assets to the wallets of a service provider. The 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. Service providers often offer more than one kind of wallet service, allowing users to take advantage of both self-custody (see paragraphs [ ] above) and custodial wallet solutions because the two different types of wallets serve different purposes.

A Trading Account

20. A (a business) offers what it terms a "Trading Account," which is the functionality within a wallet that enables a user to buy and hold all digital assets purchased with fiat currency through A The contract between A and its client expressly provides that title to the digital assets in the Trading Account remains with the user and does not transfer to A, and emphasises that digital assets in the trading account are not the property of A and are not loaned to A. A segregates digital assets in the trading account from its own assets in the entries in its own ledger, even though the digital assets may not be segregated by blockchain address. Some transactions between A's clients initiated from a trading account occur off chain, and are recorded only by accounting ledger entries in the records of A. A transaction between a self-custody wallet (provided by A or by another service provider) and a Trading Account provided by A, on the other hand, would occur on-chain.

(5) The relationship between the custodian and the client may exist notwithstanding that the client may be acting in any capacity on behalf of a third party in relation to the digital asset.

Commentary

21. Principle 11(5) makes it clear that, without affecting the existence or operation of the custody relationship, the client could be acting on behalf of a third party in any capacity. This could cover situations such as agency or nomineeship,and could also include where the client (in the relevant jurisdiction) holds the asset on trust for someone else (e.g. the client could be an investment fund or an individual holding the asset for a family member) or that the functional equivalent could occur in other jurisdictions.

Principle 12: 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 transfer the digital asset, or use it for its own benefit, except to the extent permitted by the client and other law;

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

(c) the custodian is obliged to safeguard the digital asset.

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

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

(a) the duty to keep a record of the digital assets it maintains for each client;

(b) the duty at all times to securely and effectively maintain digital assets in accordance with the records it keeps 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 maintained for the account of clients separate from assets maintained 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 maintains that asset.

(4) Where authorised by a client or by other law, a custodian may fulfil its duties to its client under a custody agreement in relation to a digital asset by entering into a custody agreement with a sub-custodian with respect to that asset if the sub-custodian is bound by the duties set out in this Principle.

(5) A digital asset maintained by a custodian for a client may be subject to a security right

(a) granted to that custodian by the client; or

(b) in favour of that custodian arising by operation of other law; or

(c) granted to a third party by the client.

Commentary

1. Principle 12(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 custody agreement. If the custodian is a sub-custodian, the client is itself a custodian.

2. 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 other law (as defined in Principle 2(4)). 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 other law. Other law of a state may permit a custodian to

have a limited right of use in relation to assets in relation to which it provides custody services: this permission may be contained in regulation and/or in private law. In the latter case, the extent of the permission may depend on the way in which a custody relationship is characterised by that private law. [It is unlikely that other law would permit a custodian to have a completely unrestricted right of use in relation to such assets.]

3. The duty in sub-paragraph (b) makes the basic point that a custodian is a person who must deal with the asset 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 12(5)).

4. Sub-paragraph (c) makes it clear that the custodian must owe to the client some duties in relation to safeguarding of the digital asset.The details of these duties will typically be included in the custody agreement. A state can choose which safeguarding duties cannot be excluded by agreement. Some suggestions are contained in Principle 12(3).

5. The language of Principle 12(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 or other type of legal relationship in other jurisdictions.

6. Principle 12(2) addresses the common situation where a service provider, such as an exchange, maintains 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 as relating to a particular client. Instead, the number of assets the custodian maintains 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. The reference to 'a custodian' in Principle 12(2) also applies to a sub-custodian, whose clients are custodians.

7. Principle 12(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. Again, it should be recalled that if the custodian is a sub-custodian, the client is a custodian.

8. The duty in sub-paragraph (a) is that a custodian must keep a record of the digital assets it maintains for every client. That record may either be kept separately from 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 maintain assets correlating to those records. Thus, if the record shows that a custodian maintains 1 BTC for A, the custodian must maintain at least 1 BTC.

9. The duty in sub-paragraph (c) is to replace any missing assets, in other words, to reconcile what the custodian actually maintains 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 maintains assets for a number of clients. A segregated account would be where a custodian maintains a number of assets 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 maintained in a segregated account.

The legal effect of the segregation described in this paragraph will depend on the applicable other law, and may vary from jurisdiction to jurisdiction.

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 12(4) makes it clear that a sub-custody structure, as explained above, especially in paragraphs 2 and 5 of the commentary to Principle 11, can be used.

13. Principle 12(5) permits a custodian to have a security right in the asset it maintains for a client. For example, 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 asset. A security right under sub-paragraph 5(a) would be made effective against third parties by control under Principle 15(1), since the custodian either controls the digital asset itself or has entered into a custody agreement with a sub-custodian in relation to the asset. A client can also grant a security right in an asset maintained by a custodian to a third party (this follows from the nature of a digital asset set out in Principles 3(1) and 14(1), but in that case the security right would need to be made effective against third parties by a means (available under other law) other than control under Principle 17(1).

Principle 13: Insolvency of custodian

(1) If a custodian enters into any insolvency proceeding, a digital asset that it maintains on behalf of a client under a custody agreement does not form part of that custodian's assets for distribution to its creditors.

[(2) If a custodian enters any insolvency proceeding, the insolvency representative must take reasonable steps for the digital assets maintained for its client to be returned to the control of that client or of a custodian nominated by that client.

(3) Paragraphs (4) and (5) apply in the following situation:

(a) a custodian enters any insolvency proceeding, and

(b) fungible digital assets of two or more clients are maintained by the custodian in an undivided pool, and

(c) the amount of digital assets maintained by the insolvent custodian is less than the aggregate number or amount of digital assets of that description credited to the accounts of those clients.

(4) The shortfall is borne first by any digital assets of a identical type maintained by the custodian for itself.

(5) Any [remaining] shortfall shall be borne by the clients for whom the custodian maintains the digital assets in an undivided pool, in proportion to the respective number or amount of digital assets of that description credited to their accounts.]

(6) Where a custodian has entered into a custody agreement with a sub-custodian with respect to a digital asset that is the subject matter of a custody agreement between that custodian and a client:

(a) If the sub-custodian enters into any insolvency proceeding, the custodian must seek to obtain control of the digital asset from the insolvency representative, or to maintain the digital 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 asset maintained as custodian for its clients do not form part of the custodian's assets for distribution to its creditors.

Commentary

1. Principle 13(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 maintains for clients as custodian are not part of the distributed estate. If, on the other hand, a service provider is not a custodian (see the commentary to Principle 11(3)), any assets it controls will usually be part of its assets for distribution to its creditors. The effect of Principle 11(3) and Principle 11(4) is that any agreement which has the three characteristics of a custody agreement set out in Principle 11(3) will attract the consequences in Principle 13(1) unless the agreement makes it clear that this is not the case. In Principle 13(1), the 'custodian' could in fact be a sub-custodian and the 'client' could be a custodian.

2. Principle 13(2), (3) (4) and (5) give guidance as to suitable rules which should (or, in the case of Principle 13(4), could) apply in relation to digital assets if a custodian or a sub-custodian enters any

insolvency proceeding. These rules are not comprehensive; the applicable insolvency law governs all other issues that could arise in these circumstances.

3. Principle 13(2) imposes a duty on the insolvency representative to take reasonable steps so that that client can obtain the digital assets controlled for it by the custodian. The client may want to obtain control of the digital assets itself, or may want another custodian to maintain them on its behalf. The insolvency representative may need to take certain steps to achieve this result, such as obtaining the private key(s) relating to those digital assets.

4. Principle 13(3) to 13(5) deals with the situation where fungible digital assets are controlled by a custodian in a 'pooled' account (see Principle 12(2)) and there is a shortfall. In these circumstances, a state may wish to provide that the loss is first met by any digital assets of an identical type maintained by the custodian on its own account. This approach follows that of Article 25(5) of the Geneva Securities Convention, in relation to which a State can make a declaration that it is to apply in that State. Similarly, it is a policy decision for a State as to whether to adopt the rule set out in Principle 13(4).

5. Under Principle 13(5) the loss of digital assets caused by the shortfall should be borne pari passu by all the clients for whom the custodian agreed to maintain the assets in the pooled account. The approach follows that of Article 26(2) of the Geneva Securities Convention. If a State chooses to adopt the rule in Principle 13(4), then the word 'remaining', which is in square brackets in Principle 13(5), applies. Otherwise, that word is not required.

6. Principle 13(6) sets out the consequences where a digital asset is held through a sub-custodian (see Principle 12(4)) of the insolvency of a sub-custodian or a custodian. If the sub-custodian is insolvent, the custodian must seek to change control of the digital asset from the insolvent sub-custodian, either to itself or to another sub-custodian. If the custodian is insolvent, its rights against the sub-custodian under the custody agreement are not part of its distributable estate.

SECTION V: SECURED TRANSACTIONS

Principle 14: Secured transactions: General

(1) Digital assets can be the subject of security rights.

Commentary

1. Principle 14 builds on Principle 3(1) which states that digital assets (as defined in Principle 2(2)) can be the subject of proprietary rights. Security rights are proprietary rights, and, therefore, digital assets can be the subject of security rights. Principle 14 reflects the general principle that secured transactions regimes should enable the use of any type of movable asset as collateral. This approach allows prospective secured creditors to decide for themselves which of the digital assets have any collateral value.

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. These transactions, covered by this Section, are called "secured transactions" in the commentary to this Section. 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. Many proprietary aspects concerning security rights are governed by other law (see Principle 3(3)(c)(e)(g)). The Principles presuppose the existence of some rules, such as the requirement to notify the grantor and third parties prior to disposal of a digital asset in enforcement of a security right, and explain how those rules would operate in the context of enforcing security rights in digital assets.

3. Furthermore, the Principles are not only for those States that have implemented the UNCITRAL Model Law on Secured Transactions. Therefore, the type of transactions which fall within the category of "secured transactions" and the types of rights which fall within the term "security right" will depend on the applicable domestic law. For example, the term "secured transactions" will typically include transactions creating various types of "security rights", such as pledges, charges, or security assignments. It may also cover outright transfers: 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. Outright transfers of digital assets may be used in various contexts (see illustration [ ]). it is therefore is important that its secured transactions law should be coordinated with its generally applicable rules governing outright transfers of digital assets.

4. In adopting these Principles, a State may need 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, thus carving out digital assets from the broader corpus of "intangible assets" to which generally applicable rules of secured transactions laws would already apply (e.g., third-party effectiveness by registration only). This would complement any existing definitions of special types of assets (e.g., deposit accounts) for which asset-specific rules have been provided for in a State's secured transactions law (e.g., third-party effectiveness may be achieved by control).

5. Where a digital asset is linked to another asset ("the other asset"), that other asset may well fall within a specific category in the domestic law of a State, such as a category of "securities"

(bearing in mind that the existence and legal effect of the link is a matter for other law, see Principle 4). The nature of the link itself may, as a matter of other law, result in the linked digital asset falling within a specific category, such as that of negotiable documents/instruments (see paragraph 10 below and commentary to Principle 4 paragraph 15 illustration 3.) In these situations, the secured transactions rules specific to that type of asset will apply to the other asset or to the digital asset itself as appropriate. A number of these rules have been designed with reference to the specific nature of an asset or the structure of the system in which it is transacted, which could cause challenges in determining how those rules are to be applied in the context of security rights in linked digital assets.

6. 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 distinctive rules could apply to various categories of linked digital assets. States should not attempt to provide for secured transactions rules specific to many categories of linked digital assets that would result in a complicated system. The concept of control set out in Principle 6 should apply equally to the third-party effectiveness of security rights in all types of digital assets (linked and non-linked).

7. The Principles in this Section address certain aspects of third-party effectiveness, priority and enforcement relating to security rights over digital assets. The rules determining the applicable law to these aspects of secured transactions are set out in Principle 5. However, there will be many aspects of secured transactions that are governed by other law (that is, domestic law that is not Principles law).

Illustration

8. The secured transactions law of State X does not carve out digital assets from the broader category of intangible assets. Control is a recognised mechanism for making a security right effective against third parties, but is available only for bank accounts and intermediated securities. The secured creditor may thus need to register to make its security right effective against third parties. Upon implementation of these Principles, the registration would be a redundant step in terms of providing public notice to third parties as the secured creditor would be in control of the digital asset (as defined in Principle 6).

(2) 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.

(3) 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.

Commentary

9. Paragraphs (2) and (3) reflect Principle 4 which provides that the existence of, requirements for and legal consequences of any link between a digital asset and another asset (either a real-world asset or a digital asset) are a matter for other law. If the link between a digital and a real-world asset is recognised under other law, for instance, as operating 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. This approach is consistent with, for instance, Article 16 of the UNCITRAL Model Law that provides for the creation of a security right in a negotiable document that may extend to goods. However, it does not define a negotiable document, which is not a matter of secured transactions law. Furthermore, these two paragraphs follow the approach of Article 17 of the UNCITRAL Model Law under which a security right in an asset does not extend to an "associated asset", such as a security right in intellectual property does not extend to a tangible asset with respect to which intellectual property is used. Accordingly, if some

other law does not establish a link between the two assets, the creation of a security right in one of the two assets would not affect the other asset. The situation could also be converse where a security right is taken in a real-world asset that is purported to be linked to a digital asset. Since these Principles deal with digital assets only, this situation is not covered. Principle 4 provides for the general approach to linked assets, which Principles 14(2) and (3) articulate in the context of creating security rights and making them effective against third parties.

Illustration

10. In State X, an invoice is not seen as an embodiment of the underlying right to payment.

    a. Factor A regularly takes control of digital invoices for due diligence purposes. This would not create a security right in the receivable nor make it effective against third parties.

    b. Factor B regularly takes a security right over receivables owed under invoices which are issued in the form of digital assets. The security right is made effective against third parties. This would not create a security right in the digital assets i.e., digital invoices nor make it effective against third parties. Though, in practice, because there is no effective link between the receivable and invoice, a security right over the digital invoice would not have any value similarly to a security right in a paper-invoice that does not embody a right to payment.

Principle 15: Control as a method of achieving third party effectiveness

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 maintains the digital asset for the secured creditor.

Commentary

1. Principle 15 provides that, in addition to any other methods of third-party effectiveness that apply to a security right in a digital asset under the other law, a State should recognise that a security right in a digital asset may be made effective against third parties by control. This would apply in a situation where the secured creditor controls the digital asset, but also where a custodian controls the digital asset on behalf of the secured creditor, including through a sub-custodian. Third-party effectiveness generally requires a secured creditor to take a step to publicise its security right, which may, for example, include delivery of possession , notification of the obligor), registration, and control . Some of these methods are not applicable to digital assets (e.g., delivery of possession of a tangible object).

2. While in most States registration would generally render a security right in most (or all) types of assets effective against third parties (e.g., in all movable assets covered by the UNCITRAL Model Law), 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 for security rights, 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. 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 already be recognised as a method to make the security right in the digital asset effective against third parties. A transfer to a wallet held by the secured creditor or its agent would then be sufficient to protect the security right against third-party claims, including in insolvency. Under laws that do not recognise such steps, the failure to register a notice may be fatal for the secured creditor. In any case, the existing requirements for third-party effectiveness may create uncertainty for those who take digital assets as collateral.

4. Secured transactions and related laws may already provide for change of control over an asset to be sufficient to transfer it, whether outright or by way of security. For instance, a State might have implemented the UNCITRAL Model Law on Electronic Transferable Records that provides for a transfer of an electronic transferable record, that may for instance be a promissory note, by control. Control may be established through i) the secured creditor obtaining control of the digital asset itself, as described in the previous paragraph (ii) a custodian maintaining the digital asset on behalf of the secured creditor; iii) the mere fact that the secured creditor is the custodian (since the custodian will then have control). Where laws already recognise 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. For example, this might be the case of digital assets linked to securities held with securities intermediaries. However, there are likely to be many other types of digital assets for which control mechanisms have not been provided for in secured transactions laws.

5. In the past, 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 prevailing practices in "crypto-lending" do not rely on registration and other traditional methods of achieving third-party effectiveness. A State should incorporate "control" as defined in Principle 6 in its secured transactions law to allow secured creditors to make their security right in digital assets effective against third parties. Incorporation of control may affect the structure of its priority rules, which is explored below in Principle 16 on priority as well as facilitate enforcement, which is explored in Principle 17.

6. A State should include the definition of control from Principle 6 in its secured transactions law (or refer to such a definition included elsewhere in its law relating to digital assets) to achieve third-party effectiveness 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. Principle 15 (1) (in conjunction with Principle 6(3)) provides that the secured creditor may exercise the requisite powers directly, through a third party custodian or in cooperation with other parties, such as in a multi-sig arrangement (see commentary to Principle 6 paragraph 12) [cross-reference to a paragraph that explains multi-sig].

7. Recognition of control in a secured transactions law consistent with this principle could result in a situation where the applicable law provides for multiple methods of third-party effectiveness. 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, a security right may be made effective against third parties by one of those methods. This principle does not preclude a State from designating control as the sole method of third-party effectiveness with respect to security rights in digital assets, consistently with its general secured transactions law (e.g., that law may provide for control as the sole method of third-party effectiveness with respect to security rights in deposit accounts).

8. There are three situations in which control under these Principles may be used to make the security right effective against third parties. First, the secured creditor may acquire the requisite powers prescribed in Principle 6. Second, the secured creditor may share these powers with other parties, which would also constitute control under Principle 6. Third, a party that is currently in control (e.g., a custodian) and/or is expected to acquire control over digital assets in the future may agree to exercise the relevant abilities on behalf of the secured creditor.

9. Principle 6 allows the abilities set out in Principles 6(1)(a) to be shared by multiple parties without compromising the existence of control (Principle 6(3)). In the context of making a security right effective against third parties, the way in which abilities are shared and the degree of sharing between the secured creditor and grantor required for the law to recognise that control continues to exist may vary from State to State. In a situation where the secured creditor and the debtor share the abilities in Principle 6(1)(a) (the third situation referred to in paragraph 8 above), while in some States it may be sufficient for the secured creditor to be in a position to exercise control when the debtor defaults, thus the debtor retaining the abilities until that point, other States may require that the abilities be transferred entirely to the secured creditor. This is a policy choice of the State. However, if the secured creditor cannot exercise the abilities without the consent, or participation of the grantor, then it should not be in control for the purpose of achieving third-party effectiveness. If the grantor has the ability to dispose on its own and the secured creditor cannot dispose without the consent of the grantor that likewise should not constitute control.

10. Although specific rules may have already been provided in some States prescribing control for some assets, such as electronic transferable records, a State should ensure that the existing criteria are sufficient to accommodate collateralisation of these records issued and transferred 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 6 for transfers of "electronic transferable records", including achieving third-party effectiveness of a security right.

11. ***Illustration 1***: In State A, which has not adopted the Principles, a secured creditor takes a non-possessory pledge over a portfolio of 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 required its borrower to transfer the relevant digital asset to a third-party wallet controlled by the secured creditor through a multi-signature arrangement but does not make a registration. Later, the borrower files for insolvency. The secured creditor could lose its security right as it was not made effective against third parties. On similar facts, in State B which has adopted the principles into its law, the secured creditor would have made its security right effective on the borrower's insolvency by control.

13. ***Illustration 2:*** Digital assets are maintained by a custodian on behalf of a customer. The custodian undertakes to exercise the control abilities on behalf of the secured creditor . If the State has incorporated "control" as a method of third-party effectiveness in its secured transactions regime, the security right will be effective against third parties.

Principle 16: Priority of security rights in digital assets

A security right in a digital asset that is made effective against third parties by control in accordance with Principle 15 has priority over a security right in the digital asset that is made effective against third parties only by a method other control.

Commentary

1. Principle 16 addresses the situation where one secured creditor has made its security right effective against third parties by registration or another method recognised by the applicable law, but has not obtained control of the digital asset, and another secured creditor has made its security right effective by control (pursuant to Principle 15). In this situation, the latter would have priority even if it took the steps to obtain control after the former made its registration or otherwise made its security right effective against third parties. This is in contrast to the general rule (under the UNCITRAL Model Law and in many States), which is that 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 (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.

2. This approach, applied to digital assets by Principle 16, is typically justified in a number of ways. First, providing for the non-temporal priority recognises that the secured creditor that took the additional steps was relying to a greater extent on the encumbered asset. This is similar to a situation where a secured creditor takes possession of a negotiable document, which would give it priority over a security right made effective against third parties by registration, under some domestic regimes. Second, the secured creditor who made its security right effective against third parties by control would not need to search the registry. Again, this is similar to the position in relation to other assets, such as negotiable instruments, in that a party taking possession is not expected to search a registry, which reduces the cost of dealing with the asset and enhances its negotiability. Moreover, it is often not practical for a secured creditor taking security over a digital asset to search the registry. For transactions with digital assets, the prospective secured creditor might not even know which registry to search as the transferor, or its identity or its location, might be unknown. Third, this priority 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. Fourth, it aligns the priority position with the position on default, when the secured creditor in control is best placed to enforce the security right, and provides an incentive for secured creditors to place themselves in this favourable position. By giving a secured creditor the ability to do this, the rule contributes to market certainty. Moreover, the approach in Principle 16 is consistent with the secured transactions rules in international instruments, 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.

3. In most States, other law has conferred some degree of transferability, typically negotiability, on some assets that allows transferees to cut off security rights made effective against third parties by registration. For instance, a transferee of money takes free of a security right if it takes possession of money without knowledge that it violates the rights of a secured creditor. A transferee is defined in these Principles to include a secured creditor (see Principle 2). Since these Principles confer a high degree of negotiability on digital assets, their transferees (including acting as secured creditors, see

Principle 2(5)) will be able to benefit from the same approach, set out in Principle 8. Most secured creditors would be expected to satisfy the requirements of the innocent acquisition principle, including acting in good faith, without any disqualifying knowledge and extending value. This is particularly true because, as described above, secured creditor that makes its security right effective against third parties by control will not be expected to search any secured transactions register.

4. 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. This situation may arise when the digital asset is held by a custodian who agrees to control the digital asset for multiple secured creditors. Generally, the two creditors would be expected to regulate their respective priority in a subordination/intercreditor agreement. In the absence of an agreement, the priority conflict may be determined based on the general priority rule contained in the applicable secured transactions law, which reflects the first-in-time principle ie, the secured creditor who obtained an acknowledgment of the custodian first would have priority.

Illustration

5. 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 has control over the virtual currency. The custodian 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 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.

Principle 17: Enforcement of security rights in digital assets

(1) Enforcement of a security right in a digital asset is subject to other law, including any requirement to proceed in a commercially reasonable manner.

(2) If a security right in a digital asset held by a custodian is made effective against third parties other than by control, the secured creditor is entitled to enforce its security right only pursuant to a court order, unless the custodian agrees otherwise.

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. Principle 17 does not prescribe particular enforcement methods for security rights in digital assets. Generally available methods provided under other law would apply. This commentary provides guidance to States as to how existing enforcement rules, such as those included in Chapter VII of the UNCITRAL Model Law, 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. As explained above in the commentary to Principle 14, this Section does not recommend changes to the characterisation of secured transactions under the applicable law. In some cases in the enforcement of rights, thus, the applicable other law may impose no, or lower, requirements on secured creditors that have acquired a digital asset outright.

3. All enforcement actions, including disposal, collection of payment (if the right to payment of a monetary obligation is the 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 accordance with the applicable enforcement rules contained in a general secured transactions law, including requirements to proceed in a commercially reasonable manner, provide notifications, distribute any proceeds in accordance with the priority rules, etc. Otherwise, the secured creditor may be liable for damages under other law. In some cases, the inherent design of the digital asset may prevent the exercise of certain enforcement rights. General rules governing enforcement of security rights 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 a number of considerations, which are set out in this commentary.

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. Furthermore, control might have been transferred to another secured creditor who would have priority (see Principle 16). The general enforcement rules of the secured transactions law then determine whether and how a senior secured creditor may take over the enforcement process.

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 to affected parties. However, secured transactions laws may also provide that under certain situations these requirements 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 would, 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 if these exceptions were crafted broadly to accommodate future developments. Some States also have bespoke enforcement procedures for specific types of assets which do not include any notification requirements (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 this Principle 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. The recognition of exceptions from the generally applicable enforcement provisions facilitates automated enforcement. 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. Many system designers are not aware of how the secured transactions enforcement rules apply. Even if systems have been designed to fit within any exceptions from the general enforcement provisions, the secured creditor must still proceed in a commercially reasonable manner.

7. Courts may need some guidance on the interpretation of any exceptions to the enforcement requirement when it comes to digital assets. For instance, in relation to one of the exceptions mentioned in paragraph 5, a "recognised market" is one in which the items sold are fungible and prices are not subject to individual negotiation, such as stock or commodity exchanges. The intended goals of the recognised market exceptions is to facilitate the efficiencies and cost savings that the special treatment may provide without disadvantaging affected parties. Although a recognised market need not be subject to regulation or supervision, the existence of regulatory requirements or guidelines may provide useful guidance for applying this exception. The test whether or not the market would qualify for the exception is a functional one. It is not based on the "type" of market. These are some of the parameters that would determine whether some exchange for digital assets actually qualifies as a recognised market.

8. If a custodian maintains the digital asset on behalf of the grantor, extra-judicial enforcement will entail action by that custodian on the instructions of the secured creditor. An intermediary will be unwilling to follow those instructions if the secured creditor is unknown and many secured transactions laws include provisions protecting intermediaries 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 17(2) provides for the protection of custodians of digital assets in the enforcement of a security right. Accordingly, if the security right has been made effective against third parties by control under Principle 15(1), the custodian would typically owe some duties to the secured creditor, including to change control of the digital assets if instructed by the secured creditor

(see Principle 12(1)(b)). In contrast, if the security right has been made effective by a method other than control, such as by registration, the custodian would not owe any duties to that secured creditor. In those situations, the secured creditor may need to obtain a court order.

Illustrations

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. However, any requirements under the other law as to acceptance of the collateral in satisfaction of the obligation would continue to apply.

SECTION VI: ENFORCEMENT

Principle 18: 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:

SECTION VII: INSOLVENCY

Principle 19: Effect of Insolvency on Proprietary Rights in Digital Assets

(1) A proprietary right [or interest] in a digital asset that has become effective against third parties under Principles law or other law is effective against the insolvency representative and creditors and any other third party 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 an asset that is part of the insolvency estate or under the supervision of the insolvency representative.

Commentary

1. Principle 19 deals with the effect of insolvency on a proprietary right in a digital asset. Principle 3(1) says that "Digital assets can be the subject of proprietary rights, (…)", which means that a person who has a proprietary right in a digital asset can assert that right against third parties, if it has been made effective against third parties. Principle 19 confirms that a proprietary right in a digital asset which is effective against third parties is effective against relevant parties in any insolvency proceeding. As explained below, the subject of the insolvency proceeding ("the debtor") may be the person who has the proprietary right or it may be another person.

2. Apart from situations falling within the innocent acquisition rule in Principle 8 and the rule in Principle 15 whereby a security right can be made effective against third parties by control, Principle 3(3) establishes that whether a person has a proprietary right in a digital asset and whether a proprietary right in a digital asset has been made effective against third parties is a matter of "other law" (that is, any part of a State's law that is not Principles law (Principle 2(4))). Principle 19(1) provides for the pre-insolvency effectiveness to continue in insolvency proceedings: the precise result of that effectiveness will also depend on the circumstances and on the applicable other law. In general, however, as recommended by the UNCITRAL Legislative Guide on Insolvency Law (2004) pages 75 – 82, the debtor's estate will comprise assets of the debtor, which are those in which the debtor has a proprietary right, to the extent of that proprietary right.

3. The consequences of the operation of this Principle can be illustrated by considering three typical situations. (1) The insolvency of a person who 'owns' a digital asset; (2) insolvency of a person, who, as a debtor, has granted to its creditor a security right in a digital asset as collateral; and (3) insolvency of a custodian, who controls a digital asset for a client. The client will wish to retrieve its digital asset. Principle 19 primarily concerns situations (1) and (2), which are considered in paragraphs 4-6 below, which, by way of example, illustrate the operation of Principle 21 in the context of insolvency proceedings resulting in a distribution to creditors. Situation (3) (insolvency of a custodian) is considered specifically in Principle 13 and the commentary to that Principle. Insolvency of a sub-custodian is covered by Principle 13(4).

4. Situation (1) can arise in at least two variations. In the first variation of situation (1) a person owns and controls a digital asset, for example, by using wallet software as a form of 'self-

custody' (see paragraphs 11-13 of the commentary to Principle 11). When this person becomes insolvent, the digital asset forms part of that person's estate, since the person's proprietary right remains effective on insolvency (Principle 1(1)). Under typical insolvency law, the insolvency representative can infringe upon an insolvent person's proprietary rights in that she can exercise an insolvent person's proprietary rights for the benefit of that insolvent person's creditors. Thus, the insolvency representative may assume control over the insolvent person's digital assets, sell those assets and distribute the proceeds amongst the creditors. Notably, 'control' here is used in a broad sense, and not as defined in Principle 6. Therefore, in situation (1), the insolvency representative is likely to want to retrieve the digital asset, and sell it for the benefit of the insolvent person's creditors. Taking control of the digital asset, however, may not be straightforward, compared to taking control of other types of assets. Access to the wallet and/or the private key is likely to be passworded, and the insolvent person might refuse to reveal the password. Whether (and how) the insolvency representative can obtain a court order against the insolvent person ordering him to reveal the password will depend on the applicable insolvency law.

5. The second variation of situation (1) is where the insolvent person has a proprietary right in the digital asset but the asset is maintained for him by a custodian. The insolvent person's proprietary right is effective despite the insolvency proceedings, and the insolvency representative, as above, will want to retrieve and sell the digital asset. This time, it is easier for the insolvency representative, since if the applicable insolvency law allows her to take control of the insolvent person's assets, she will be able to instruct the custodian to transfer the asset to her control or to a third party to whom she has agreed to sell the asset.

6. There are also a number of variations of situation (2). In the first variation, a person owns and controls a digital asset in some sort of self-custody arrangement (see paragraphs 11-13 of the commentary to Principle 11). That person has granted a security right in the digital asset to his creditor. On that person's insolvency, the creditor may wish to enforce the security right in the digital asset during the debtor's insolvency. Under Principle 19(1) the creditor's security right is not affected by the insolvency. This means that (depending on the applicable insolvency law and concrete situation) the security right can be enforced by the creditor or the insolvency representative can realise the value of the asset and pay the creditor out of this value. In any event, the creditor's security right will have the same effect as a security right in any other asset (which will depend on the applicable insolvency law, see, for example, paragraph 10 below), but the same possible difficulties about obtaining control of the asset mentioned above will occur. The same analysis applies if the digital asset is maintained by a custodian for the insolvent person, except that unless the custodian has agreed to act on the instructions of the secured creditor, a court order will typically be required (see Principle 17(2)). If the secured creditor has taken control of the digital asset, it is much easier for it to enforce the security right extra-judicially (see commentary to Principle 17 paragraph 4), but whether it can do so will depend on the applicable insolvency law.

7. While Principle 19 is meant to leave a person's proprietary rights in a digital asset unaffected by insolvency, this protection is not absolute (see also Principle 5(3) and (4)) For example, the application of a State's other law may result in the preference of another person's rights over the relevant digital asset. Principle 19(1) does not affect the operation of a such a rule, whether it is substantive or procedural, providing that it applies by virtue of the insolvency proceedings. These rules may be found in any part of a State's law that is not Principles law (i.e. that is "other law" as defined in Principle 2(4)), including its tax law, insolvency law, general private law and its procedural law. Principle 19(2) lists three examples of instances where the relevant rules of a State's other law may affect the rights of creditors, which are not affected by Principle 19(1).

8. The first example, set out in Principle 19(2)(a), concerns the ranking of categories of claims. An applicable State's law governing the priority order in which claims on the insolvent estate or on specific assets forming part of the estate are to be ranked, will typically dictate that certain categories of creditors have preference over other creditors (including secured creditors). For example, a State's

law may prescribe that fiscal authorities have priority over secured and unsecured creditors in relation to certain assets of the insolvent person, or that the costs of the insolvency proceedings have preferential status over other secured and unsecured creditors' claims on the insolvent estate.

9. The second example, set out in Principle 19(2)(b), concerns the fraudulent transfer of assets. Under the applicable State's insolvency or private law, a transfer of ownership of digital assets may typically be rescinded by the transferor's insolvency representative, if the transfer was made in a prescribed period prior to the insolvency and if the transferor transferred the digital assets to defraud its (other) creditors. Thus, a State's insolvency or private law may infringe upon the proprietary right in a digital asset of a person who has acquired that digital asset. Similarly, the applicable insolvency or private law may enable a transfer of digital assets amounting to a 'preference' to be rescinded by the insolvency representative of the transferor, if certain conditions are fulfilled.

10. The third example, set out in Principle 19(2)(c), clarifies that, if the insolvency representative has taken 'control' of the digital asset as described in paragraph 4 above, Principle 19(1) does not affect the operation of any rule of the applicable law relating to the enforcement of rights to that asset [whether by the insolvency representative or anyone else]. For example, a rule providing for a stay on enforcement by a secured creditor would not be affected by Principle 19(1). [Principle 19(2)(c), read in conjunction with Principle 19(1), therefore also implies that third parties, including the network or system that operates the (record of the) digital assets in question, must acknowledge and accommodate the insolvency representative's exercise of the insolvent person's rights in these digital assets. See also Principle 13.]