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

EN

Digital Assets and Private Law Working Group

Fifth session (hybrid)
Rome, 7 – 9 March 2022

UNIDROIT 2022
Study LXXXII – W.G.5 – Doc. 3

English only
February 2022

MASTER COPY OF THE PRINCIPLES AND COMMENTS

Table of contents

General question

Q.1. *Bearing in mind the importance of technology neutrality, and bearing in mind the rapid development of new technologies and business models in the digital realm, which approach to the Commentary would the Working Group recommend be taken:*

- *Should more examples be provided in the commentary, given the technical complexity of the subject matter? One possibility is that the commentary could be periodically updated in order to ensure that technological and industry developments have not run so far ahead as to render the examples given obsolete.*

OR

- *Should the commentary aim to provide only a limited number of concrete examples and illustrations, given that those examples risk becoming rapidly outdated?*

INTRODUCTION

I. REASONS FOR THE *PRINCIPLES*

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.

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

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.

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.

II. RELATIONSHIP OF *PRINCIPLES* TO NATIONAL LAW

These Principles apply certain core concepts (described below) and do not attempt to address all contractual and proprietary issues relating to the digital assets covered by the Principles. As States may have a wide range of other laws (in statutes and court decisions), there is no attempt to identify the specific law that may apply.

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

III. *SCOPE OF PRINCIPLES*

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). 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).**

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

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: Digital Assets 'linked' to other assets**).

IV. CORE CONCEPTS

Proprietary aspects. These Principles treat digital assets as having proprietary characteristics, without addressing whether they are considered 'property' under the other law of a State.

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

Control. As discussed above in connection with the description of which digital assets are addressed by this law, the concept of 'control' plays a critical role in these rules (see discussion of transfer below).

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

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.

V. TRANSITION RULES

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.

Questions regarding Introduction

Q.2. *With regard to the current draft introduction, and bearing in mind its purpose to provide a broad overview of the reasons for and scope of the Principles:*

- *Are there any key elements which are missing?*
- *Are there any elements which merit further elaboration?*

Q.3. *Should the introduction elaborate further upon why digital assets require special private law rules?*

SECTION I: SCOPE AND DEFINITIONS

Question

Q.4. *How should the problem of classification of digital assets as objects of proprietary rights be addressed (particularly to avoid forcing States to create a separate category for digital assets)?*

Principle 1: Scope [of the principles]

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

Commentary

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

2. These Principles take a practical and functional approach in that they are intended to facilitate the private law treatment of digital assets in both common law and civil law systems. They are not jurisdiction specific, and can be applied to any legal system or culture. They address situations where gaps may exist in current law, and also where traditional approaches would not be appropriate and should be modified.[2] However, as is made clear in the Principles and commentary, there are many issues of private law which are not addressed by the Principles. The internationality of the Principles will enable jurisdictions to take a common approach to legal issues arising out of the holding, transfer and use of digital assets across a variety of use cases.[3]

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

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

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

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

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

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

Principle 2: Definitions

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

1. 'Electronic records' comprise a class of which 'digital assets' (as defined in principle 2(2) form a subset. As defined, an 'electronic record' consists of information stored in an electronic or other intangible medium, which is capable of being retrieved. It is implicit in the requirement that the information be retrievable that the information also must be retrievable in a form that can be perceived. It follows that an electronic record would not include, for example, oral communications that are not stored or preserved or information that is retained only through human memory.

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

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

3. The definition of 'digital asset' includes an electronic record only if it is 'capable of being subject to control'—as 'control' is defined in Principle 6. For example, some electronic records might be described colloquially as 'digital assets', but normally could not be subjected to 'control', as defined, and consequently would not be digital assets as defined here.

4. Consider a simplified example: Two sets of information compose an electronic record. One set is 'No Left Turn Unstoned' (NLTU) *plus* information (key information) that, pursuant to public-key cryptography, renders this set of information capable of being subject to control by means of the associated private key. (Note that this does not mean that the key information necessarily contains the private key itself, but only the information that makes it controllable with the private key.) Those two components—NLTU plus the key information—compose the digital asset (the 'NLTU digital asset'). The second set of information is 'I Gave Her the Ring, She Gave Me the Finger' (IGHTR, SGMTF). Although information consisting of IGHTR, SGMTF is associated with and included in the same electronic record as the NLTU digital asset, a transfer of control of the NLTU digital asset so that it becomes subject to control through different key information would not transfer control of the IGHTR, SGMTF information. Indeed, the IGHTR, SGMTF information is not (it is assumed) capable of being subject to control. This example is not unrealistic. For example, an interest in Bitcoin is composed of an unspent transaction output (UTXO). The UTXO might be associated with information, such as information included in a header, that is a part of the same electronic record as the UTXO but which is not capable of being subject to control. The header information would not necessarily be transferred as a result of spending the UTXO.[6]

---

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

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

5. Continuing with the example of the NLTU digital asset described in comment 2, pursuant to Principle 9 an innocent acquirer (IA) of the NLTU digital asset would acquire it free of conflicting proprietary claims. But this would not mean that the IA acquires the information NLTU (e.g., that the IA 'owns' NLTU). Instead, the IA acquires the information NLTU only insofar as it is associated with the key information as a part of the NLTU digital asset. The information NLTU itself presumably exists not only as a component of the NLTU digital asset but also independently and separate and apart from the NLTU digital asset. The information NLTU is the same—'No Left Turn Unstoned' is 'No Left Turn Unstoned'—however or wherever that information might be stored, existing, or perceived. The NLTU digital asset is distinct, however, because it is composed not onlyof the information NLTU *but also of the key information*.

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

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

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

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

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

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

---

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

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

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

If the information included in the digital asset is itself subject to protection under intellectual property law (presumably copyright law, in this example), the rights of the holder of the intellectual property would be preserved notwithstanding the inclusion of the information in theelectronic 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 beentitled to the use and enjoyment of the information (not unlike the lawful purchaser of a bookprotected 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'srights by using the information.

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

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

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

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

Illustration 4: Facebook page with password for access.

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

Illustration 5: Excel or Word file with password protection.

A Word, Excel or similar data file 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 knowledge of the password would have the exclusive abilities necessary to obtain control under Principle 6. Because the file would be capable of being subject to control, the file would be a digital asset as defined in Principle 2(2) and within the scope of these Principles. That said, unless the digital asset were associated with a protocol that facilitates the acquisition and disposition of such assets, laws adopting these Principles would not have any material utility or impact for these assets. One might view this circumstance as indicating that the scope of the Principles is overbroad. However, it is

better characterized as merely an example of digital assets that would not normally be disposed of and consequently would not benefit from or involve the need for the legal regimes that the Principles contemplate. On the other hand, an attempt to narrow the definition of digital asset to exclude such digital assets might risk the exclusion of assets that would (or could) benefit from inclusion.

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

(4) 'The law' means a State's law including its digital assets law.

Commentary

8. Under Principle 1, these Principles cover private law issues relating to digital assets. Therefore, these Principles provide rules for issues such as the custody and transfer of, and the provision of security interests in digital assets. Under this definition (3), all the rules provided by the Principles qualify as 'digital assets law' once they have been adopted and implemented into a State's law. Notably, these Principles take no position as to whether [its rules] [they] should be included in a State's special law on digital assets, incorporated into more general laws, already follow from general laws, or are addressed by a combination of these approaches.

9. 'Digital assets law' may or may not already follow from general private law rules in a specific jurisdiction. [However, the law should specify which (if any) of its existing rules or standards of general application cover digital assets whenever controversial, specifically where it concerns the acquisition and disposition of proprietary rights in digital assets. Notably, if a State's law includes classification of different types of property or assets which can be subject to proprietary rights which have different consequences, that law should specify which type or types of property digital assets are.][8] See also the commentary to Principle 3(1) below.

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

Questions

Q.5. *In light of the broad colloquial meaning given to the term 'digital asset', the Working Group may wish to consider whether another term, perhaps one that is more functionally oriented or more closely associated with the concept of control, should be employed to confine the scope of these Principles. Consideration might be given, for example, to 'transferable digital asset' (cf. 'electronic transferable record', defined in Article 2 of the UNCITRAL Model Law) or 'controllable digital asset'.*

Q.6. *What other key terms ought to be defined in this principle, e.g. custody, transfer, fungibility, etc.?*

Q.7. *Should we add definitions of 'the other law', 'other than DA law', 'applicable law', or 'material law'?*

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

Principle 3: General principles

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

Commentary

1. Under Principle 1, these Principles cover private law issues and in particular proprietary rights relating to digital assets. This Principle 3(1) therefore provides, as a matter of principle, that the law (as defined under Principle 2(4)) should provide that digital assets can be the subject of proprietary rights. All rules provided in these Principles are built on this premiss. However, the question whether digital assets can be the subject of proprietary rights has been controversial in several jurisdictions. As courts in multiple high profile cases have considered that digital assets are the subject of proprietary rights, and several authoritative authors have expressed that digital assets *should* be the subject of proprietary rights,[9] these Principles advise States to end legal uncertainty on this issue and make explicit that digital assets can be the subject of proprietary rights. 'Proprietary rights' is defined in principle 3(2).

2. That States should provide that digital assets can be the subject of proprietary rights also means that if a State's law includes classification of different types of property or assets which can be subject to proprietary rights which have different consequences, that law should specify which type or types of property digital assets are.

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

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

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

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

(3) The law other than digital assets law continues to apply to issues not dealt with in these Principles, including

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

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

---

9 [sources to be added]

(c) whether a person has validly created a security right in a digital asset;

(d) the rights as between a transferor and transferee of a digital asset;

(e) the rights as between a grantor of a security right in a digital asset and the relevant secured creditor

(f) the legal consequences of third party effectiveness of a transfer of digital assets; and

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

Commentary

6. This Principle 3(3) makes explicit that other law, i.e. all law within a given State that is not 'digital assets law' as defined in Principle 2(3), continues to apply to digital assets. For this purpose, this Principle 3(3) lists several examples of issues of property law, but also of contract law, that may continue to be regulated by a State's other law, because these Principles do not cover those issues, nor do they intend to change or derogate from that other law. The list is not intended to be exhaustive or limitative.

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

8. Second, Principles 3(3)(b) and (c) concern dynamic situations of acquisition and disposition of digital assets from the perspective of the transferor and security right provider, respectively. If the question arises whether a person has validly transferred a proprietary right, or validly created a security right in a digital asset, these Principles 3(3)(b) and (c) make it clear that the requirements for a (valid) transfer and creation of a security interest continue to be, as a matter of principle, a matter of other law. [However, these Principles do provide for specific issues regarding the transfer of, and creation of a security interest in digital assets: these provisions are then 'digital assets law', which takes precedence over other law.] [These issues are then covered by the Principles, which is considered 'digital assets law' and takes precedence over 'other law'] Principle 16(2), for instance, provides that a State's law should provide distinct rules in relation to creation of a security right and effectiveness against third parties for one or more types of digital assets where their individual features and characteristics are such that the application of specific rules, distinct from those applying to intangible assets generally, would be necessary.]

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

10. As explained above, Principles 3(3)(d) and (e) concern the (contractual) relationships between a transferor and transferee, and between a provider of a security right and the relevant

secured creditor, respectively. These provisions thus concern *inter se* relationships, i.e. relationships between (contracting) parties. Principles 3(3)(f) and (g), on the other hand, concern *erga omnes* relationships, i.e. the relationships with third parties. Pursuant to these Principles 3(3)(f) and (g), whether a transfer and a creation of a security interest, respectively, can be asserted against third parties, continue to be, as a matter of principle, a matter of other law. In several jurisdictions, the 'assertability' of a right or interest against third parties follows from the concept of 'effectiveness'. These Principles 3(3)(f) and (g) provide that, whatever the dogmatic context, the requirements for such effectiveness or assertability continue to be, as a matter of principle, a matter of other law. However, these Principles do provide for specific issues regarding the effects of proprietary rights or interest in digital assets. [These provisions are then 'digital assets law', which takes precedence over other law.] [These issues are then covered by the Principles, which is considered 'digital assets law' and takes precedence over 'other law'.] Principle 17, for instance, provides that a State's law might provide distinct rules in relation to the effectiveness of a security right in digital assets.

Questions

Q.8. *Should the commentary provide some guidance on the introduction of the digital assets law and its interaction with the existing law (for example, EU Member States' experience implementing EU directives)?*

Q.9. *Does the Working Group agree with the commentary to Principle 2(4) and Principle 3(1) indicating that the law should specify which, if any, of the existing rules or standards of general application govern proprietary rights relating to digital assets?*

Principle 4: Digital Assets 'Linked' to Other Assets

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

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

Alternative formulation for discussion:

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

Commentary

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

2. The principle makes clear that the legal effect of the link (if any) is not addressed in these principles, in particular because: (i) the nature of the link may vary from case to case depending on the facts and on the law, and (ii) the issue of proprietary rights in the 'other asset' is a matter that is to be determined in accordance with the law applicable to that asset (paragraph 1). 'Legal effect' means any type of legal effect, including, most importantly, questions as to the enforceability of

acquisitions and dispositions, including their enforceability in insolvency. [The principle confirms that 'the law' is a State's law other than the 'digital assets law' (defined Principle 2(3)).]

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

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

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

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

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

Examples of 'linked' assets:

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

Illustration 1: The general law already in force may recognise that the parties' transaction with the digital asset on the blockchain ledger is legally effective to change the state of proprietary rights in the other asset off the ledger.

For example, a system may be established for trading quantities of tokenised gold [e.g. PAX Gold]. An investor who buys a token from the issuer acquires a proprietary right in a fractional share of specifically identified gold. A sale and transfer of the token may pass the seller's proprietary right in the gold to the buyer. The link between the token and the gold is legally effective if the general law treats the parties' dealings with the token as the outward expression of their intention to transfer the proprietary right in the gold.

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

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

Illustration 3: The precise legal effect of any link between the digital asset and the other asset may depend as much on ascertaining the parties' intentions from any system coding, protocols and documentation as it does from the operation of the general law. Thus the terms of a White Paper

accompanying the issue of digital asset may be relevant to inferring the nature and value of the legal right, if any, that the holder of the digital asset was intended to have in relation the other asset.

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

The terms of the White Paper show that each holder of the coin was primarily intended to have a contractual right against the issuer. It would, however, be for the insolvency law of the relevant state to determine how, if at all, this right might take priority over any other claims of general creditors of the issuer.

Illustration 4: Digital assets may be used to create transferable portions of value derived from other assets which exist off the blockchain. The precise ascertainment of the holders' rights may be determined – and limited – by the general law of the state.

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 law where the company is registered, or the real estate is located. The relevance of the digital asset is to illustrate: (i) the 'chain' of ownership between the holder and the shares and the real estate; and (ii) steps that may need to be taken by the acquirer of the token (and depending on the law and administrative practices of the jurisdiction concerned) to update a company register; or update a register of real estate.

This illustration shows that the mere fact of the transfer of the token from one person to another may not be enough by itself to perfect the transfer of ownership of the real estate, nor may the existence of the token be sufficient to prevent the transfer of the real estate from one person to another.

[Note further examples to be inserted e.g. tokenised bonds: here, the issuing document specifies that the principle and coupon are owed only to the holder of the digital asset. In some cases this will be supplemented by a provision that the debt obligation cannot be transferred to a person unless the token is also transferred]

Questions

Q.10. *Does the Working Group agree to leave the requirements for documentation demonstrating the link between the assets to the scope of regulation of the other law or the law? Is Principle 4(2) satisfactory to achieve this goal?*

Q.11. *In a static situation of custody, would the holding of a digital asset have an effect on the other linked asset?*

Q.12. *Could the Working Group provide additional examples (to be included in the commentary) of linked assets of various types; particularly, stablecoins and NFTs?*

Q.13. *What apart from the digital asset itself should be referred to in Principle 4(1) as a possible source of the appearance of linkage between the assets?*

SECTION II: PRIVATE INTERNATIONAL LAW

Principle 5 – Conflict of Laws [10]

1) General principle

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

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

2) Determination of the applicable law

The law applicable to proprietary questions in digital assets

a) The law applicable to propriety questions in respect of digital assets is identical for all digital assets of the same description.

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

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

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

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

f) If no law has been chosen in respect of the relevant [network] [system] the law of the State to which the [network] [system] has the strongest factual connection applies, in particular in cases in which the network operator is resident, incorporated or regulated or has otherwise a clear factual connection to a specific State.

3) Recognition in insolvency

Notwithstanding the opening of an insolvency proceeding, the law applicable in accordance with the previous rules governs all proprietary aspects in respect of digital assets with regard to any event that has occurred before the opening of that insolvency proceeding.

---

[10] 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.

Commentary

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

2. Paragraph (2) deals with the determination of the law applicable to proprietary questions in relation to digital assets. There are three important aspects: (a) the law is chosen uniformly for all assets of a specific issue, (b) it should be a visible (not secret) choice, (c) assets of different issues can be stored and transacted on the same system, cf Ethereum. The law of the asset and the law of the system may be the same or it may be different.

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

Questions

Q.14. *Does the Working Group agree that the implementation of this principle should include the rule for the choice of law according to the example we provide in the principle?*

Q.15. *In what way should party autonomy be fixed in the principle?*

Q.16. *Does the Working Group agree that a prescriptive rule ought to be formulated that the issuer should determine the law for the digital asset in an express manner?*

Q.17. *Does the Working Group agree with the substance of the rules set out in Principle 5? In particular, with regard to:*

- *The default rule set out in paragraphs 2(a) to (c)?*
- *The substance of paragraph 2(d)?*
- *The fallback provisions in paragraphs 2(e) and (f)?*

Q.18. *Does the Working Group agree with the rule on recognition in insolvency in paragraph 3?*

SECTION III: CONTROL

Principle 6: Definition of Control

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

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

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

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

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

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

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

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

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

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

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

- The exclusive ability requirements in paragraph (1)(a) of this Principle (as relaxed in paragraph (3)) 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. The exclusivity criterion of control (including the standards for its relaxation) appears to reflect the norm in the relevant markets for digital assets. Acquirers expect and believe that they have obtained the relevant exclusive abilities with respect to a digital asset (subject to understood exceptions) and in fact that generally has been the case.

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

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

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

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

Explanation and commentary

'Ability' of a person with control

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

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

Exclusivity of abilities

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

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

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

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

Illustrations of the application of Principle 6 (definition of 'control')

Illustration 1: Shared control and multi-sig arrangements.

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

Principle 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 paragraph (1)(b) is satisfied as to the abilities specified in Principle 6 paragraph 1(a)[(i) and (ii)];

(b) it is not necessary for that person to prove that no person other than the person in control and those permitted by paragraph (3) has any of the abilities specified in Principle 6 paragraph 1(a).

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

Commentary

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

control may demonstrate that it has a better proprietary interest than the person currently in control by proving that the change of control was wrongful.

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.

SECTION IV: TRANSFER

Question

Q.19. *Could the Working Group provide additional examples for the commentary of the transfer of digital assets, in particular, of the on-chain and off-chain transfers and transfers involving the Layer-1 and Layer-2 digital assets?*

Principle 8: Acquisition and Disposition of Digital Assets

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

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

Commentary

Paragraph (1) addresses not only the transfer of a digital asset from one person to another person but a transfer that results in the acquisition of a derivative digital asset that is not the same digital asset that was disposed of by the transferor. An example of such a derivative digital asset is the UTXO (unspent transaction output) generated by a transaction in Bitcoin. Another example might be adjustments in balances in accounts resulting from transactions in ether on the Ethereum platform, as to which the digital asset that is disposed of and the digital asset that is acquired are fungible assets and not necessarily the "same" asset.[11]

Principle 9: Innocent Acquirer Rule

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

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

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

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

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

(4) The innocent acquirer rule should provide that

(a) an innocent acquirer takes a digital asset free of conflicting proprietary rights ("proprietary claims");

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

(b) no rights based on a proprietary claim relating to a digital asset may be successfully asserted against an innocent acquirer of that digital asset;

(c) Control of a digital asset should be an essential element for qualifying as an innocent acquirer; and

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

Commentary

1. The rights conferred on IAs in accordance with subparagraphs (a) and (b) of paragraph (4) 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 (4) is intended to make clear that, for example, even if an acquirer receives control of a digital asset by a change in control made by a thief or a hacker, the acquirer may qualify as an IA. See also the discussion in Principle 6, Explanation and commentary, paragraph 3.

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

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

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

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

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

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

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

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

(h) the test adopted in the Geneva Securities Convention, Article 18(1), i.e., whether:

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

(6) If an innocent acquirer rule provides that qualification as an innocent acquirer requires the absence of notice or knowledge, the law should specify the effect of a transferee's notice or knowledge, including its impact on the claims as to which a transferee does and does not take free.

Principle 10: Shelter principle

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

Principle 11: Application of Innocent Acquirer Rules to a Custody Relationship

[The law should provide that] A client that acquires a proprietary right in a digital asset through a custody relationship with a custodian

(a) takes its right free of conflicting proprietary claims, or

(b) that no rights may be asserted against the client based on a conflicting proprietary claim, or

(c) both (a) and (b),

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

Commentary

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

SECTION V: CUSTODY

Principle 12: Custody

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

Commentary

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

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

(2) In this Section

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

[(b) a custodian holds a digital asset if

(i) that custodian controls the digital asset, or

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

Commentary

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

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

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

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

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

(c) the client does not have the exclusive ability to change the control of the digital asset;

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

Commentary

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

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

Question

Q.20. *Bearing in mind the private law nature of these Principles, what aspects of the relationship between the custodian and the client would the Working Group consider ought to be further elaborated?*

Principle 13: Duties owed by a Custodian to its Client

(1) A custodian owes the following duties to its client:

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

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

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

Commentary

1. The language of Principle 13(1) is intended to be functional and neutral between legal cultures. In some jurisdictions, the custodian/client relationship will be legally characterisedas a trust while it may be characterised as a contractual relationship in other jurisdictions.

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

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

4. The duty in sub-paragraph (b) makes the basic point that a custodian is a person who must deal with the assets according to the client's instructions.

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

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

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

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

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

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

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

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

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

Commentary

7. The duty in sub-paragraph (a) is that a custodian must maintain a record of the digital assets it holds for every client. That record may either be maintained separately of the distributed ledgers which record the respective digital assets or, if technology allows, be part of the information stored in the distributed ledger. The duty in sub-paragraph (b) is that the custodian owes a duty to hold assets correlating to those records. Thus, if the record shows that a custodian holds 1 BTC for A, the custodian must control at least 1 BTC.

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

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

10. 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.

Questions

Q.21. *Does the Working Group agree that all the various entities and technical arrangements present in the provision of custodian services for digital assets ought to be considered as custodians under these Principles?*

Q.22. *Furthermore, are they all able to comply technologically with all the duties?*

Q.23. *How would the Working Group recommend addressing those situations where the mandatory duties cannot be performed by some DeFi structures, for example, Maker DAO?*

Q.24. *Could the Working Group provide additional examples of models of custody of digital assets (for the purposes of the commentary)?*

Principle 14: Other Aspects of Custodianship

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

Commentary

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

(2) A digital asset held by a custodian for a client

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

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

Commentary

2. Principle 14(2) permits a custodian to have a security interest in the asset it controls for a client. The client may owe the custodian fees, for which the custodian wishes to be secured, or the custodian may have lent the client money to acquire the assets.[12]

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

Commentary

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

Principle 15: Sub-Custody

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

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

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

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

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

Examples

Examples of custody

[description of 'pure' custody]

[description of an exchange]

[description of custody of a 'tethered' asset]

Examples of situation which are not custody

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

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

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

however, should not alter the legal characterisation of the obligation as a personal right or its treatment as an unsecured claim in the bankruptcy of the obligee.]

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

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

SECTION VI: COLLATERAL TRANSACTIONS

Principle 16: Collateral Transactions: General

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

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

Commentary

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

Illustrations

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

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

Notes

Some secured transactions regimes may enable the use of any movable property as collateral, while others specify the types of property that may be encumbered (e.g., equipment, but not inventory of a business, may be subject to an enterprise charge under some laws). The former, whether statutory or judge-made, may define a security right as a "property right in a movable asset", without defining "movable asset".[13] Applicable law defines what constitutes a movable asset. Some laws allow the creation of an interest with respect to anything that can be traded, including intangible assets.[14] Although actions, claims or rights may be listed as an example of an incorporeal asset in the relevant statutory provision, typically it is not clear whether digital assets would be covered. In principle, under these regimes, an interest may be created in any incorporeal asset, including digital assets. However, an explicit statutory treatment would in this case provide greater legal certainty.

---

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

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

(2) The law should provide distinct rules in relation to creation of a security right and effectiveness against third parties for digital assets where their individual features and characteristics are such that the application of specific rules, distinct from those applying to intangible assets generally, would be necessary.

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

Commentary

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

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

Illustrations

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

(4) 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 the law and is not covered in these principles.

(5) 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 the law and is not covered in these principles.

Question

Q.25. *How should the Principles ensure a jurisdictionally neutral explanation regarding collateral?*

Principle 17: Control as a Method of Achieving Third Party Effectiveness

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

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

(i) those set out in Principle 6 (1)(a)(i) and (iii) ("positive control") or

(ii) that set out in Principle 6 (1)(a)(ii) ("negative control") or

(iii) those set out in Principle 6(1)(a)(i), (ii) and (iii) ("negative and positive control").

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

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

(b) a custodian is itself the secured creditor.

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

Commentary

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

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

3. Market participants generally take some steps to preclude the borrower from accessing the encumbered digital asset, typically by transferring it from the wallet of a borrower to a wallet, or under the control (e.g., in a multi-signature arrangement), of the secured creditor. Under some laws those steps may be recognized as a mechanism to make the security rights effective against third parties. A transfer to a wallet held by the secured creditor or its agent should be sufficient to protect the security right against third-party claims, including in insolvency. For instance, a security transfer

of ownership may be effective against third parties upon executing of an agreement to that effect. For digital assets that may be encumbered under this device, the creditor might not need to take any additional step to make its security right effective against third parties. In contrast, in some regimes the failure to register a notice may be fatal for the secured creditor, as no other mechanism might exist to achieve third-party effectiveness of a security right in a digital asset. In any case, the existing requirements for third-party effectiveness create uncertainty for market participants.

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

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

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

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

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

Illustrations

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

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

Principle 18: Priority of Security Rights in Digital Assets

(1) [The law should provide that] [W][w]here a security right in a digital asset has been made effective against third parties by through control, the security right should have priority over a security right in the digital asset of a person that does not have control.

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

Commentary

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

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

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

Furthermore, Principle 9(4)(a) generally cuts off any conflicting proprietary claims. The secured creditor acquiring control is expected to satisfy the other requirements to qualify as an innocent acquirer.

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

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

Illustration

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

Principle 19: Effective Enforcement of Security Rights in Digital Assets

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

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

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

Commentary

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

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

3. All enforcement actions, including disposal, collection of payment (if monetary obligation is the main characteristic of a digital asset) and acceptance of the collateral, in full or partial satisfaction of the secured obligation, should be available. In enforcing their rights, secured creditors

must proceed in a commercially reasonable manner and satisfy certain conditions that balance the interest of affected third parties. The inherent design of the digital asset may prevent exercising certain enforcement rights. General rules governing enforcement, typically included in international standards on secured transactions appear to be flexible enough to accommodate the expectation of digital assets lenders and other relevant parties. However, States should take into account several considerations.

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

5. Second, secured transactions laws balance the interest of affected parties by imposing certain requirements on secured creditors, such as to provide notifications. However, under certain situation these requirements may not apply. For instance, Article 78(8) of the UNCITRAL Model Law provides for exceptions from the requirement to provide a notification when the asset may speedily decline in value or is sold on a recognized market. These kinds of exceptions should arguably apply to many digital assets (e.g., Bitcoin may speedily decline in value while stablecoins may not, and some NFTs may already trade on recognized markets while others do not). Enforcement provisions in secured transactions laws may not need to be changed to accommodate digital assets as these exceptions were generally crafted broadly to accommodate future developments. For those digital assets that qualify as intermediated securities (e.g., upon their credit to a securities account), any notification requirements may not apply at all.[15])

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

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

Illustration

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

---

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

control of the secured creditor resulting in the acceptance of the collateral in satisfaction of the secured obligation or enabling a foreclosure sale.

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

SECTION VII: ENFORCEMENT

Question

Q.26. *What, in the opinion of the Working Group, should be the content and scope of the enforcement principle?*

SECTION VIII: INSOLVENCY

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

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

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

(a) the ranking of categories of claims;

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

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

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

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

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

Commentary

1. The insolvency law should recognise the third-party effectiveness and priority of a security right and should not impair it for the sole reason that the collateral is a digital asset. The insolvency law should not impose any further requirement to establish or maintain the third-party effectiveness of a security right established prior to the insolvency proceedings.[16]

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

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

---

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

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

4. Valuation of assets affects recovery of secured creditors in an insolvency proceeding. It also impacts other aspects of secured transactions, including determination of the amount to be lent and distribution of proceeds upon disposition of the collateral. Insolvency laws do not provide specific guidance on the valuation method to be used, such as the "going concern value" or the "liquidation value". Currently, there are no standardized valuation approaches which creates uncertainty for secured creditors as to the value they may be able to receive. Given these challenges, it might be useful to explore and assess whether and how the existing valuation standards and methods apply to digital assets,[17] focusing on the rights of secured creditors in insolvency. This may be particularly necessary for digital assets that do not have a value that may be readily established for instance through a secondary market. Such assets may include some NFTs and utility tokens, the value of which is not necessarily determined by supply and demand and thus, may require different ways to measure the value; for instance, by comparing them to similar ones. Valuation of "digital twins" may present peculiar challenges as well. The international standards could offer guidance as to which valuation approaches and methods to apply to digital assets, in accordance with their classification. On the contrary, valuation of digital assets, such as CBDCs, stablecoins, and other virtual currencies might be more straightforward but it could still benefit from further guidance.

5. Considering the diversity of rights and obligations associated with digital assets, the choice of the valuation approach may highly depend on the classification of the digital asset and its intended purpose. Besides, different valuation approaches may provide different results as the inputs used may vary. In specific circumstances involving certain digital assets, one valuation approach may be more appropriate than the others. Methodologies for the valuation of digital assets started to emerge, drawing on those applicable to intellectual property.[18] This is particularly relevant for those digital assets linked to an intellectual property right (e.g. NFTs associated with art).

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

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

---

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

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

Illustrations

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

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

Questions

Q.27. *What, in the opinion of the Working Group, should be the content and scope of the insolvency principle?*

Q.28. *Which of the two alternatives presented in the draft principle does the Working Group consider to be preferable?*