UNIDROIT PRINCIPLES ON DIGITAL ASSETS AND PRIVATE LAW

UNIDROIT

UNIDROIT

International Institute for the Unification of Private Law

UNIDROIT PRINCIPLES ON DIGITAL ASSETS AND PRIVATE LAW

Suggested form of citation:

UNIDROIT Digital Assets and Private Law Principle 2(2)

Published by the
International Institute for the Unification of Private Law (UNIDROIT)
Via Panisperna, 28 - 00184 Rome - ITALY

ISBN: 978-88-86449-49-6

FOREWORD

- I -

Introducing a new instrument is always a reason for celebration. After years – for years it takes – of sowing, the time to harvest the crop arrives and, with it, the actual realisation of our mandate. A new instrument marks the successful ending of a process where considerable effort and resources have been spent. Few projects have required as much effort – and used as many resources – as the Principles on Digital Assets and Private Law. A new topic covering a new reality which moves at a speed which is difficult to make compatible with the usual timing of transnational law, and which is fundamentally at odds with the carefully pondered, slow motion of Government interaction as well as with the complex debates involving experts with a global membership, each potentially with a diverse vision of reality. In addition to the speed at which the conception and use of digital assets may potentially mutate, the unpredictable evolution of technology presented another layer of complexity.

Staving off all those risks was a challenge which had to inform the approach to the instrument. This explains the search for a technology-neutral, legal system-neutral, jurisdictionally agnostic solution to the fascinating legal problems encountered in the process. This instrument is not a solution for a given moment and for a specific technology, but a thorough analysis of the main private law issues that could arise when dealing with digital assets in the market. It is essentially a transactional instrument, which seeks to assist legislators and users in solving the complexities that concern the proprietary use of digital assets.

A classic transnational law instrument codifies best practices. An initial step of this codification consists of identifying those legal regimes that have proved to work better in practice. This project was also different in this regard. The novelty of the subject matter was such that no specific private law rules had emerged, anywhere, as the better solution. Hence, the discussion at the Working Group level was in good part an original attempt at creating – not merely identifying – an international standard on the proprietary aspects of digital assets. UNIDROIT has served, thus, as the venue where experts from all representative legal families and systems converged to determine the most adequate solutions, an extraordinary service to the international legal community. This explains, naturally, the prudent approach adopted by the Principles, which only cover those areas where the nature and characteristics of digital assets required legal clarification or where ad hoc solutions were demanded. The rest – the majority – of private law matters are left to domestic law, although, even where reference is made to "other law" (as it is

called), helpful guidance and legal analysis is provided in the Commentary, a part of the instrument which is almost as important as the blackletter Principles themselves. Rather than providing a comprehensive, new private law framework, the purpose of the instrument is to fill existing gaps and add legal certainty in the application to digital assets of a pre-existing national private law regime.

- II -

The General Assembly of UNIDROIT, at its 79th session (Rome/Zoom, 17 December 2020) assigned the highest level of priority to the project for the development of an international instrument on digital assets and private law. On this basis, a Working Group on Digital Assets and Private Law was established by UNIDROIT. The Working Group was composed of 16 Members with expertise in private law, technology law, and commercial law, as well as 52 Institutional Observers from 28 international, governmental, industry, regional, and non-governmental organisations, and 10 Individual Observers. Given the enormous interest raised by the project, a Steering Committee was set up as an additional body to channel input reflecting the special context and circumstances of the Institute's global constituency. The Committee was composed of representatives of 27 UNIDROIT Member States and one Regional Economic Integration Organisation, who provided input on the documents issued by the Working Group as they were being produced.

The Working Group held nine sessions between November 2020 and March 2023. Under the guidance of the Drafting Committee, the Working Group prepared a set of Draft Principles on Digital Assets and Private Law which embody best practices and international standards, enabling jurisdictions to take a common approach to legal issues arising from the transfer and use of digital assets. The Steering Committee was consulted twice during the Working Group's deliberations. Finally, the Secretariat conducted a public online consultation in which 44 sets of comments were received, including 341 individual comments and one position paper from the European Association of Private International Law (EAPIL).

These Principles are hence the result of over three years of intensive research, deliberations, and consultations, which led to their final adoption by the UNIDROIT Governing Council at its 102nd session (10-12 May 2023).[1]

1 UNIDROIT 2023 – C.D. (102) 25, paras 92-106.

- III -

UNIDROIT would like to express its deepest gratitude to the Members and Observers of the Working Group, to the participants of the Steering Committee, and to those who contributed to the public online consultation. The success of this project would not have been possible without their outstanding competence and personal commitment.

Particular mention is deserved by Professor Hideki Kanda, Member of the UNIDROIT Governing Council, who masterfully chaired the Working Group. His generous personal effort constituted an example which, together with his unrivalled 'auctoritas', was instrumental in ensuring the hard intersessional work generously granted to the project by so many world-class experts. An enormous debt of gratitude is also owed to Professor Louise Gullifer, who served as the Chair of the Working Group's Drafting Committee, and whose knowledge and energy proved an essential part of the project's success. In fact, all members of the Drafting Committee must be specially thanked for their efforts and dedication to this project.

A special word of thanks also goes to Ms Marina Schneider for the extensive work done in preparing the French version of the Principles, to Mr Hamza Hameed who managed this project on behalf of the UNIDROIT Secretariat in its final and decisive stage, to Mr Carlo Di Nicola, who initially led the project for the Secretariat, and to Ms Audrey Chaunac and Ms Isabelle Dubois, for whose secretarial support the project is greatly indebted.

The UNIDROIT Principles on Digital Assets and Private Law have already become the basis of law reform proposals regarding digital assets in different parts of the world, and will offer guidance to legislators, judicial officers, and all stakeholders in the digital economy, which is becoming an increasingly important part of economic discourse and development.

Ignacio Tirado
UNIDROIT Secretary-General

Maria Chiara Malaguti
UNIDROIT President

September 2023

UNIDROIT PRINCIPLES ON DIGITAL ASSETS AND PRIVATE LAW

CONTENTS

INTRODUCTION

I. REASONS FOR THE PRINCIPLES

0.1. These Principles are designed to facilitate transactions in digital assets of the type covered by the Principles, which are defined in Principle 2(2). These are types of digital assets often used in commerce.

0.2. For transactions in these types of digital assets to have the maximum efficiency, it is important to have clear rules that apply to the key aspects of these transactions (briefly described in Commentary 0.13 to 0.19). Without predictable results, the transactions will have inherent inefficiencies and there will be greater costs and a reduction in the value of the transactions in commerce.

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

0.4. It is recommended that States adopt legislation consistent with these Principles. This will have several benefits. It will increase the predictability of transactions involving these assets that occur in those States. In addition, as these transactions frequently involve persons in different States, the greater the consistency among States, the greater the predictability in cross-border transactions. The increased predictability should reduce the costs of these transactions, both in direct transaction costs and pricing.

II. NEUTRALITY AND THE RELATIONSHIP OF THE PRINCIPLES TO NATIONAL LAW

0.5. These Principles take a practical and functional approach. This has several important effects. First, these Principles are technology

and business model neutral. In several instances the Commentary to these Principles refers to, and uses examples that draw on, distributed ledger technology such as blockchain technology. However, this has been done only to clarify the application of the Principles and is not meant to favour assets that employ these types of technology, or to modify or undermine the applicability of these Principles to digital assets that employ other technologies. Importantly, this is not meant to impair the technology neutrality of these Principles. Thus, these Principles are intended to apply to all digital assets (as defined in Principle 2(2)), whether or not the record of these digital assets is on a blockchain. On the scope of these Principles, and more specifically, the type(s) of digital assets these Principles cover, see Commentary 0.11 and 0.12 and Principle 1.

0.6. Second, these Principles are jurisdiction neutral. Therefore, they have not been drafted using the terminology of a specific jurisdiction or legal system and are intended to be applied to any legal system or culture. This means that they are intended to facilitate the legal treatment of digital assets in all jurisdictions, including common law and civil law systems. The concept of control used in these Principles, for instance, is not intended to be understood as 'control' as used in certain common law jurisdictions. Also, while being akin to the concept of 'possession' as used in certain civil law jurisdictions, control as used in these Principles must not be understood to be identical to such possession: where in civil law jurisdictions a possessor may 'hold' an asset through another person, under these Principles a person cannot control a digital asset through another person unless the criteria set out in Principle 6 or agency law are met (see Commentary 6.6).

0.7. The jurisdiction neutrality of these Principles as explained above also means that it is for the jurisdiction in question to decide how to implement these Principles into its own law(s) and legal system. Traditionally, common and civil law jurisdictions use different approaches to address new phenomena and to implement supra-national law, and these Principles do not prescribe a specific approach. A jurisdiction, for instance, may elect to adopt a specific statute that is consistent with, or implements, these Principles as a whole. Alternatively, another jurisdiction may elect to implement these Principles into existing law and amend it as appropriate. These

Principles thus take no position as to whether their rules should be included in a State's special law on digital assets, should be incorporated into more general laws, already follow from general laws, or are to be addressed by a combination of these approaches.

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

0.9. The organisational neutrality of these Principles also does not mean that they are intended to be implemented outside of private law. These Principles cover only private law issues relating to digital assets and, in particular, proprietary rights. Thus, they specifically address digital assets where these are the object of dispositions and acquisitions, and where interests in those assets are to be asserted against third parties. As a matter of principle, they do not cover rules that are to be enforced by public authorities which in many jurisdictions would be called 'regulation' or 'regulatory law'. For instance, these Principles do not cover such matters as when, or whether, a person must obtain a licence for engaging in activities that concern digital assets. However, jurisdictions may wish to adopt rules of 'regulatory law', *i.e.*, rules that are to be enforced by public authorities, to accompany and operate in tandem with these Principles. For instance, States may wish to adopt rules that prescribe how an offeror of a digital asset must disclose that that digital asset is linked to another asset (if any). See Principle 4 and its Commentary for a discussion of linked assets. Should the offeror breach these rules, the relevant supervisory authority could typically sanction that breach

by imposing a fine or revoking the offeror's licence. Also, States may wish to adopt rules that prescribe how a custodian of digital assets must segregate the digital assets it maintains for clients from its own assets. These rules may concern both the manner in which the custodian must operationally administrate client assets, and the legal method through which it must achieve that client assets do not form part of that custodian's assets available for distribution to its creditors if the custodian enters into an insolvency-related proceeding. See Principle 11(3)(d) (for the private law duty), Commentary 11.8 and Principle 13(2). Again, should the custodian breach these rules, the relevant supervisory authority could typically sanction that breach by imposing a fine or revoking the custodian's licence.

0.10. Moreover, these Principles intend to cover only a specific area of private law, and there are many issues of private law which are not addressed by the Principles. These issues concern, for instance, rules of private law relating to intellectual property or consumer protection. As a matter of principle, these areas of law are not addressed by these Principles, and national intellectual property and consumer protection laws therefore remain unaffected by them. Also, these Principles do not address many issues of national private law relating to contract and property law. Examples of these issues not addressed by these Principles include whether a proprietary right in a digital asset has been validly transferred to another person, whether a security right in a digital asset has been validly created, the rights as between a transferor and transferee of a digital asset, the rights as between a grantor of a security right in a digital asset and the relevant secured creditor, many of the legal consequences of third-party effectiveness of a transfer of digital assets and some of the requirements for, and legal consequences of, third-party effectiveness of a security right in a digital asset (see also Principle 3(3) and Principle 4). In sum, these Principles establish certain core concepts and rules (described in Commentary 0.13 to 0.19) and do not attempt to address all contractual and proprietary issues relating to the digital assets covered by the Principles. As States may have a wide range of other laws (in statutes and court decisions), there is no attempt to identify the specific law that may apply.

III. SCOPE OF THE PRINCIPLES

0.11. These Principles apply only to a subset of digital assets. They are distinguished from other digital assets by identifying them as digital assets that are capable of being subject to control (as briefly discussed in Commentary 0.15) (see Principle 2(2)). For these Principles, 'control' refers to a digital asset where a person can establish that it has (i) the exclusive ability to prevent others from obtaining substantially all of the benefit from the digital asset, (ii) the ability to obtain substantially all the benefit from the digital asset and (iii) the exclusive ability to change the control of the digital asset to another person. See Principle 6.

0.12. In some cases a digital asset covered by the Principles will state that it is 'linked' to another asset. As discussed in Commentary 0.10 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.

IV. CORE CONCEPTS AND RULES

Proprietary aspects

0.13. These Principles establish that digital assets (as defined in Principle 2(2)) are susceptible to being the subject of proprietary rights, without addressing whether they are considered 'property' under the other law of a State. See Principle 1 and Principle 3(1). As being the subject of proprietary rights, it is appropriate to fashion rules applicable to digital assets that provide for the protection of innocent acquirers and for security rights in digital assets, taking into account the particular characteristics of a digital asset. See Principle 8 and Principle 14.

Private international law

0.14. Given the intangible nature of 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 types of connecting factors that are often relevant to determining applicable law for tangible objects are not suitable to be used in this context.

Instead, the Principles give significant effect to party autonomy in this regard, and allow for the digital asset itself, or the system on which the digital asset is recorded, to specify expressly the law that governs proprietary issues with respect to the digital asset, as well as providing for other connecting factors in particular circumstances. These other factors include, where there is an 'issuer' (as defined in Principle 5(2)(f)) of the digital asset, the location of the issuer's statutory seat. For the custody issues addressed in Principles 10 to 13, the law provided in the custody agreement applies to those issues. See Principle 5.

Control

0.15. The Principles have developed a concept of 'control', consisting of a number of factual abilities that a person must have in order to have control of the digital asset, as discussed in Commentary 0.11. The concept of 'control' plays a critical role in the rules included in the Principles, in particular for the innocent acquisition rule and making a security right effective against third parties (see discussion of transfer below), as well as for the definition of a custody agreement. See Principles 6 and 7, and Principle 10.

Transfer and secured transactions

0.16. These Principles cover the set of transactions most important in commerce – transfers of proprietary rights in a digital asset and the creation of a security right in a digital asset (see Principle 2(5)). The Principles provide some specific rules that reflect how the digital assets covered by the Principles are used in commerce, typically in 'real time' transactions (other issues relating to transfer and security rights are left up to other law, see Commentary 0.10, 1.2 and 1.3). As part of the Principles, an innocent transferee who has control and meets certain additional requirements, will take the digital asset free of proprietary claims to it (an innocent acquirer). The rights of an innocent acquirer will benefit subsequent transferees under a 'shelter' rule even if the subsequent transferee is not itself an innocent acquirer. A secured creditor can make a security right in a digital asset effective against third parties by obtaining control of the digital asset. In addition, a secured creditor who has control of a digital asset will have priority over other secured creditors with a security right in the same

digital asset who do not have control of the digital asset. Those other secured creditors would include those who have made their security right effective against third parties by registration. These rights will benefit subsequent transferees under a 'shelter' rule even if the subsequent transferee is not itself an innocent acquirer. The definition of 'control' is carefully designed to work equally well to address the rights of an innocent acquirer and as a method to make a security right in a digital asset effective against third parties. See Principles 8 to 9 and Principles 14 to 17 (Section V: Secured transactions).

Custodians

0.17. The digital assets addressed by these Principles will often be maintained by custodians. The Principles make it clear in what circumstances a person is acting as a custodian, and provide that the digital assets maintained by a custodian for clients are not part of the custodian's assets available for distribution to its creditors if the custodian enters into an insolvency-related proceeding. They also address the duties and powers of custodians in relation to those assets. Where a sub-custodian maintains a digital asset for a custodian, the Principles address that relationship in a manner comparable to the Principles that address the relationship between a custodian and its client. See Principles 10 to 13 (Section IV: Custody).

Procedural law

0.18. The Principles generally provide for the application of other law to address procedural matters, including the enforcement of rights relating to digital assets. See Principle 18.

Effect of insolvency

0.19. The Principles provide that proprietary rights that have been made effective against third parties are generally effective against an insolvency representative. See Principle 19.

V. TRANSITION RULES

0.20. If a State implements these Principles by legislation, in general they 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. For example, a secured creditor who made a security right in a digital asset effective against third parties by registration before the grace period but who failed to make that security right effective against third parties by control (see Principle 15) during the grace period might lose priority, after the end of the grace period, to a subsequent secured creditor who made its security right effective against third parties by control during the grace period.

SECTION I: SCOPE AND DEFINITIONS

Principle 1

Scope

These Principles deal with the private law relating to digital assets.

Commentary

1.1. 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 as collateral of digital assets, as defined in Principle 2(2). The Principles cover only private law issues relating to digital assets and, in particular, proprietary rights. Thus, they specifically address digital assets where these are the object of dispositions and acquisitions, and where interests in those assets are to be asserted against third parties. As a matter of principle, they do not cover rules that are to be enforced by public authorities (which in many jurisdictions would be called 'regulation' or 'regulatory law'). For instance, these Principles do not cover such matters as when or whether a person must obtain a licence for engaging in activities that concern digital assets. In the same vein, they do not cover rules for how persons should hold digital assets, if compliance with those rules is required by public authorities.

1.2. Moreover, these Principles intend to address only a specific area of private law, and there are many issues of private law which are not addressed by the Principles. These issues concern, for instance, rules of private law relating to intellectual property or consumer protection. As a matter of principle, these areas of law are not addressed by these Principles, and national intellectual property and consumer protection laws therefore remain unaffected by them. Also, these Principles do not address many issues of private law relating to contract and property law, for the reasons set out in Commentary 1.3. Examples of these issues not regulated by these Principles include whether a proprietary right in a digital asset has been validly transferred to another person, whether a security right in a digital asset

has been validly created, the rights as between a transferor and transferee of a digital asset, the rights as between a grantor of a security right in a digital asset and the relevant secured creditor, the legal consequences of third-party effectiveness of a transfer of digital assets, some of the requirements for, and legal consequences of, third-party effectiveness of a security right in a digital asset. See also Principle 3(3) and Principle 4.

1.3. These Principles address situations where gaps may exist in current (private) laws, and also where traditional approaches would not be appropriate and should be modified. However, these Principles take a practical and functional approach in that they are intended to facilitate the private law treatment of digital assets in all technological and legal systems. Thus, the internationality of the Principles will enable jurisdictions to take a common approach to legal issues arising out of the holding, transfer and use of digital assets as collateral across a variety of use cases. On the technological, jurisdiction, and organisational neutrality of these Principles, see the discussion in Commentary 0.5 to 0.9.

Principle 2

Definitions

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

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

(3) 'Principles law' means any part of a State's law which implements or is consistent with these Principles.

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

(5) In relation to a transfer of a digital asset:

(a) 'transfer' of a digital asset means the change of a proprietary right in the digital asset from one person to another person;

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

(c) 'transferor' means a person that initiates a transfer, and 'transferee' means a person to which a proprietary right is transferred;

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

(6) 'Insolvency-related proceeding' means a collective judicial or administrative proceeding, including an interim proceeding, in which, for the purpose of reorganisation or liquidation, at least one of the following applies to the assets and affairs of the debtor:

(a) they are subject to control or supervision by a court or other competent authority;

(b) the debtor's ability to administer or dispose of them is limited by law;

(c) the debtor's creditors' ability to enforce on them is limited by law.

(7) The meaning of the following terms is specified elsewhere in these Principles:

(a) 'issuer' (Principle 5(2)(f), for the purposes of Principle 5(1)(c));

(b) 'control' (Principle 6);

(c) 'change of control' (Principle 6(2));

(d) 'resulting digital asset' (Principle 6(2));

(e) 'proprietary claims' (Principle 8(2));

(f) 'custodian', 'sub-custodian', and 'client' (Principle 10(1));

(g) 'maintain' (Principle 10(2));

(h) 'custody agreement' (Principles 10(3) and 10(4));

(i) 'shortfall' (Principle 13(5)).

(8) Words in the singular include the plural and those in the plural include the singular.

Commentary

Electronic record

2.1. '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 medium, which is capable of being retrieved. 'Electronic medium' must be understood in a broad sense. Thus, the definition is intended to include any type of digital technology, even if the storage itself may not rely on

electrons, such as hard disks using magnetic fields, and DVDs using physical changes in the material. It is implicit in the requirement that the information be retrievable that the information also must be retrievable in a form that can be perceived. It follows that an electronic record would not include, for example, oral communications that are not stored or preserved or information that is retained only through human memory.

2.2. This definition is consistent with the definition of the term 'electronic record' found in various national laws, insofar as the term is defined as 'information'. Were it not for this provenance of the definition it might seem odd that the term 'electronic *record*' is defined as 'information' and not as a '*record*' of information (except as might be implicit in the requirement that the information be stored and retrievable). If one were writing on a clean slate, perhaps it would make sense to use the 'record of information' formulation. However, the role of this term is solely as a component of the definition of 'digital asset'. As explained in Commentary 2.3 to 2.17, the determinative factor is whether an 'electronic record' 'is capable of being subject to control'. It follows that either formulation of the definition of 'electronic record' would produce the same result. Therefore, the definition of the term has been chosen that already has been generally accepted.

Digital asset

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

2.4. Consider a simplified example: three sets of information compose an electronic record. One set is 'Info Alpha' and a second set is 'key information' that, pursuant to public-key cryptography, renders these two sets of information capable of being subject to

control by means of the associated private key. This does not mean, however, that the key information necessarily contains the private key itself, but only the information that makes it controllable with the private key. These two sets of information compose the digital asset 'Digital Asset Alpha'. The third set of information is 'Info Beta'. Although Info Beta is associated with and included in the same electronic record as Digital Asset Alpha, a change of control of Digital Asset Alpha so that it becomes subject to control through the different key information of the transferee would not transfer control of Info Beta. Indeed, Info Beta is not (it is assumed) capable of being subject to control. This example is not unrealistic. For example, an interest in bitcoin is composed of an unspent transaction output (UTXO). The UTXO might be associated with information, such as information included in a header, that is a part of 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. The information included in a digital asset must also be distinguished from associated information such as Info Beta or any other asset in any way linked or associated with the digital asset. Principle 4 addresses such linked assets, for example, gold or securities linked to a digital asset. See discussion in Commentary 4.13 to 4.15 and 4.21.

2.5. Continuing with the example of Digital Asset Alpha described in Commentary 2.4, pursuant to Principle 8 an innocent acquirer (X) of the Digital Asset Alpha would acquire it free of conflicting proprietary claims. But this would not mean that X acquires Info Alpha (*e.g.*, that X 'owns' Info Alpha, even if that information could be 'owned' under the applicable law). Instead, X acquires the Info Alpha only insofar as it is associated with the key information as a part of Digital Asset Alpha. Info Alpha exists not only as a component of Digital Asset Alpha but also independently and separate and apart from Digital Asset Alpha. Info Alpha is the same – 'Info Alpha' is 'Info Alpha' – however or wherever that information might be stored, existing, or perceived. Digital Asset Alpha is distinct, however, because it is composed not only of the Info Alpha *but also of the key information*.

2.6. Info Alpha might be an image, poem, book, video, song, database, a combination of 1s and 0s without any inherent value, or

any other type of information. But whatever its content or characteristics, under Principles law (see Principle 2(3), defining 'Principles law') the information would remain subject to other law. If Info Alpha were subject to valid copyright protection, for example, the rights of the holder of the copyright would not necessarily be affected by the creation, acquisition, or transfer of Digital Asset Alpha. On the other hand, it is possible that inclusion of Info Alpha in Digital Asset Alpha, or the use, transfer, or acquisition of Digital Asset Alpha, could violate, or infringe upon, rights under such laws. Even if Info Alpha (or any other information included in a digital asset) were not subject to any protection under intellectual property or other laws, the existence, use, or rights (if any) in respect of that information outside of and other than as a part of Digital Asset Alpha would not be affected by Principles law.

2.7. The information such as Info Alpha included in a digital asset must also be distinguished from associated information such as Info Beta. The following Illustrations to Principle 1 (scope), Principle 2(1) (definition of 'electronic record'), and Principle 2(2) (definition of 'digital asset') provide additional examples of the application of the definition of digital asset and the scope of these Principles.

2.8. ***Illustration 1: Virtual (crypto) currency on a public blockchain (e.g., bitcoin) is a digital asset.*** In a public blockchain no one person controls the underlying protocol (software) *i.e.*, the blockchain that tracks transactions in the digital assets. A consensus mechanism embedded in the protocol verifies the validity of transactions that users attempt to effect through the protocol. No one individual user has control over the protocol or its consensus mechanism. The underlying protocol (system) for the public blockchain itself would not be capable of being subject to 'control' (as defined in Principle 6). However, an individual user does have control over a private key, which allows the individual user to obtain 'control' (as so defined) over a digital asset within the protocol (*i.e.*, over a UTXO (unspent transaction output) in the case of bitcoin).

2.9. Although other public blockchains may differ from the bitcoin blockchain as to the applicable consensus mechanism and the manner that transactions are tracked, the foregoing description would apply nonetheless. An individual user could not, alone, control the

underlying protocol (the database or blockchain), but could control its own private key and thereby have 'control' (as defined) over the digital assets held through the protocol. A protocol within which a digital asset exists is not itself a digital asset within the scope of these Principles; however, an asset controlled by a private key is a digital asset within the scope.

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

2.11. ***Illustration 2: A CBDC may be a digital asset.*** A State wishing to issue a central bank digital currency (CBDC) could do so in a number of ways. One possibility is that the State issues a digital asset as defined in Principle 2(2). In that case, units of the CBDC could correspond to an electronic record that is subject to control as defined in Principle 6.

2.12. The relevant monetary statute of the issuing sovereign State (or monetary union) would define the legal relationship between the holder of the CBDC and the issuing central bank. It would also govern the legal nature of the CBDC as a currency, including its name and its convertibility with physical currency at par. Monetary law (*lex monetae*) would also decide whether the use of the CBDC is open to everyone (retail CBDC) or only to certain institutions (wholesale CBDC), and whether, and to what extent, it is legal tender amongst its users.

2.13. However, depending upon the CBDC's design features, and as for all digital assets (as defined in Principle 2(2)), these Principles could inform the private law rules applying to proprietary issues and transactions involving a CBDC such as a transfer from one person to another (whether as payment of a debt or as creation of a security right). Transactions in a CBDC issued in the form of a digital asset could require protection of innocent acquirers in the same way as transactions in tangible currency (see Principle 8 and Commentary 8.7).

2.14. ***Illustration 3: If a digital asset contains information that is a valuable dataset or database (e.g., a dataset that is the basis for the operation of an artificial intelligence (AI) system), image, or textual expression, the information is subject to applicable intellectual property laws and the information existing outside***

of the digital asset is not part of the digital asset. As discussed in Commentary 2.6, if the information included in the digital asset is itself subject to protection under intellectual property law (presumably copyright law, in this example), the rights of the holder of the intellectual property would be preserved notwithstanding the inclusion of the information in the electronic record or the transfer of the digital asset to an innocent acquirer. To the extent permitted by the applicable intellectual property law, the transferee of the digital asset might be entitled to the use and enjoyment of the information (not unlike the lawful purchaser of a book protected by copyright). Alternatively, if the information or its functionality were protected by patent law, for example, then the acquirer of the digital asset could be infringing the patentee's rights by using the information.

2.15. 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 Principles law and other law relating to digital assets should be subject to any applicable intellectual property laws. It also illustrates the broader point that a digital asset comprises only the package of information that includes the information necessary to make it capable of being subject to control. As discussed above in Commentary 2.4 and 2.5, the same information that is included in a digital asset, and that exists outside of and separate and apart from the digital asset, is not a part of the digital asset.

2.16. ***Illustration 4: A social media page with password for access is not a digital asset.*** Generalisations about social media or social networking platforms are difficult. But social media platforms generally involve licensing arrangements with users that do not permit the users to acquire 'ownership' of 'pages' or the data stored on the platform. This is so even though, colloquially, users may refer to 'their' pages and information that 'belongs' to them. In general, these platforms do not allow users to acquire the exclusive abilities contemplated by the definition of 'control' in Principle 6. Consequently they do not constitute or involve digital assets within the scope of these Principles.

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

or similar data file recorded in a hard drive is an electronic record as defined in Principle 2(1). If access to viewing the contents of the file is password protected, then it is possible that one who has both knowledge of the password and direct access to the hard drive in which the file is stored would have the exclusive abilities necessary to obtain control under Principle 6. Because the file would be capable of being subject to control, the file would be a digital asset as defined in Principle 2(2) and within the scope of these Principles. That said, unless the digital asset were associated with a protocol that facilitates the acquisition and disposition of such assets, Principles law would not have any material utility or impact for these assets. For example, in order to transfer control of a password protected Word file that is stored in a hard drive, it would be necessary to hand over not only the password to the file but also the hard drive in which the file is recorded. If a person in control of the file were to send the file, for example as an email attachment, to another person who is given the password, that would *not* amount to a change of control. The file received would be an entirely new electronic record – albeit an exact copy of the material information. Moreover, as discussed in Commentary 2.6, control of the file would not impair rights existing under any applicable intellectual property laws. One might view this circumstance as indicating that the scope of the Principles is overbroad. However, this circumstance is better characterised as merely an example of digital assets that would not normally be disposed of and consequently would not benefit from or involve the need for the legal regimes that the Principles contemplate. On the other hand, an attempt to narrow the definition of digital asset to exclude such digital assets might risk the exclusion of assets that would (or could) benefit from inclusion.

Principles law and other law

2.18. Under Principle 1, these Principles cover private law issues relating to digital assets. Therefore, these Principles provide rules for issues such as the custody and transfer of, and the provision of security rights in, digital assets. Under Principle 2(3), all the rules provided by the Principles qualify as 'Principles law' once they have been adopted and implemented into the law of a State. For the avoidance of doubt, 'Principles law' thus also includes the private international law rules provided in Principle 5, once these rules have

been implemented into the law of a State. Notably, these Principles take no position as to whether its rules should be included in a State's special law on digital assets, should be incorporated into more general laws, already follow from general laws, or are addressed by a combination of these approaches. On the technological, jurisdiction, and organisational neutrality of these Principles, see more extensively Commentary 0.5 to 0.9.

2.19. 'Principles law' may or may not already follow from general private law rules in a specific jurisdiction. If, in a specific jurisdiction, the law following from general private law rules is consistent with these Principles, then under these Principles such general private law rules are considered to be 'Principles law', but only to the extent they apply to digital assets as covered by these Principles.

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

2.21. More generally, if, in a specific State, it is unclear, which (if any) of its existing rules or standards of general application apply to digital assets, it is recommended that this is clarified. This is specifically relevant where it concerns the acquisition and disposition of proprietary rights in digital assets. This may also mean, for instance, that a State should specify which (if any) of its existing rules or standards of general application govern the provision of security rights in digital assets. It does not mean that the law of a State needs to list every rule or standard which applies to digital assets. Not only would this be far too complicated, it would also be unnecessary as

these Principles are concerned with private law rules only, and proprietary rights in particular. See also Commentary 3.1 to 3.4.

2.22. Within the law of a State, all law that is not 'Principles law' as defined here is referred to as 'other law' in these Principles (see Principle 2(4)). 'Principles law' and 'other law' as defined here together form 'the law'. Other law includes administrative rules and judicially determined law, as well as legislation.

Transfer

2.23. A transfer as defined here, *i.e.*, a change of a proprietary right (discussed in Commentary 3.4) in a digital asset, must be distinguished from a change of control of a digital asset (as defined in Principle 6(2)). A change of control may or may not be associated with a transfer of proprietary rights (See Commentary 2.26). In some situations, and depending on the applicable other law, a change of control will not result in a transfer of proprietary rights. A custodian (as defined in Principle 10(1)), for instance, may obtain control of a digital asset for a client, but will typically not acquire 'ownership' (as defined under the applicable national law) of that digital asset. Vice versa, whilst in many situations a transfer of proprietary rights will be accompanied by a change of control, in some situations it may not. The law of a State, for instance, may provide that under certain circumstances a proprietary right (such as ownership) in a digital asset may pass to another person, whilst control stays with the transferor.

2.24. A transfer, as defined in Principle 2(5), includes not only the transfer of a digital asset from one person to another person but a transfer that results in the acquisition of a resulting digital asset that is not the same digital asset that was transferred by the transferor (see Principle 6(2)). An example of such a resulting digital asset is the UTXO (unspent transaction output) generated by a transaction in bitcoin. Another example might be adjustments in balances in accounts resulting from transactions in ether on the Ethereum platform, as to which the digital asset that is disposed of and the digital asset that is acquired are fungible assets and not necessarily the 'same' asset.

2.25. In these Principles, the term 'transfer' is also used to denote the grant of a security right in favour of a secured creditor, and a 'transferee' includes a secured creditor. This use of the term transfer is for definitional purposes only, and does not mean that, pursuant to these Principles, a grant of a security right must be identified with a transfer of ownership or of any other proprietary right under the applicable law. See, *e.g.*, Convention of 5 July 2006 on the Law Applicable to Certain Rights in Respect of Securities held with an Intermediary ('Hague Securities Convention'), Article 1(1)(h) (defining 'disposition' as 'any transfer of title whether outright or by way of security and any grant of a security interest, whether possessory or non-possessory').

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

2.27. The term 'transferor' is defined as 'a person that initiates a transfer' because that person may have the power to transfer greater rights than that person has. Indeed, a person in control of a digital asset may have no rights at all but has the power to transfer rights to an innocent acquirer. See Principle 8(4) and Commentary 8.9.

Insolvency-related proceeding

2.28. The definition of 'insolvency-related proceeding' is not meant to provide a general definition of insolvency proceedings but defines the concept only for the purpose of these Principles. A general definition of 'insolvency proceedings' can be found in the UNCITRAL Legislative Guide on Insolvency Law and subsequent insolvency law texts. The definition in Principle 2(6) seeks to include all forms of collective, insolvency-related procedures, which may take place in court or out of court, so long as the procedure is aimed at dealing with a debtor's current or immediate financial or economic

distress and some legal effect is attached to the commencement of that procedure. This definition captures the new generation of insolvency proceedings whose legal design, often labelled as 'hybrid', features characteristics of both formal, in court proceedings and out of court contractual, collective workouts. The term 'insolvency-related proceeding', as defined in Principle 2(6), would include full in court proceedings; proceedings the opening of which entails a limitation in the debtor's ability to manage and/or dispose of its assets outside the ordinary course of its business; or proceedings which merely trigger a temporary stay of enforcement against the debtor's assets necessary for the continuation of the business activity. Hence, unlike in other legal texts such as the 2009 UNIDROIT Convention on Substantive Rules for Intermediated Securities ('Geneva Securities Convention') (Article (1)(h)), a debtor would find itself in an 'insolvency-related proceeding' for the purpose of these Principles even where its assets are not subject to control or supervision of the court or an administrative authority.

2.29. The word 'control' used in Principle 2(6)(a) must be understood in its common meaning given under insolvency law, not in the sense specified in Principle 6 of these Principles.

Other definitions

2.30. Principle 2(7) contains a list of terms used in the Principles the meaning of which is specified elsewhere in the Principles, and is for the purpose of cross-reference.

Rule of interpretation

2.31. Principle 2(8) contains a general rule of interpretation that applies to the whole of the Principles. For example, if a digital asset is generally understood to be fungible (*i.e.*, of the same description), a reference to 'a digital asset' or 'the digital asset' includes a reference to a certain quantity of digital assets of the same description, see Commentary 11.6.

Principle 3

General principles

(1) A digital asset can be the subject of proprietary rights.

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

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

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

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

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

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

(e) the rights as between a grantor of a security right in a digital asset and the secured creditor to whom the security right is granted;

(f) the legal consequences of third-party effectiveness of a transfer of a digital asset;

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

Commentary

Principle 3(1)

3.1. As stated in Principle 1, these Principles cover private law issues and, in particular, proprietary rights relating to digital assets.

Principle 3(1) therefore provides, as a matter of principle, that Principles law (as defined in Principle 2(3)) should provide that digital assets can be the subject of proprietary rights. All rules provided in these Principles are built on this premise. However, the question of 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, these Principles advise States to increase legal certainty on this issue and make explicit that digital assets can be the subject of proprietary rights. What is meant by 'proprietary rights' is discussed in Commentary 3.4.

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

3.3. Principle 3(1) also leaves to other law (as defined in Principle 2(4)) issues such as whether a person has a proprietary right in a digital asset and whether a proprietary right in a digital asset has been validly transferred to another person. Whilst Principle 3(1) does require that digital assets must be susceptible to proprietary rights, it does not prescribe, for instance, the specific requirements for a valid right of ownership in a digital asset or for a valid transfer of the same. These issues are left to other law. See also Principle 3(3) and Commentary 3.8 to 3.12.

3.4. The phrase 'proprietary rights' in these Principles is used in a broad sense, in that 'proprietary rights' include both proprietary interests and rights with proprietary effects. This broad definition reflects the functional approach of these Principles, which intend to cater for the largest variety of jurisdictions possible. Also, the definition of proprietary rights intends to express that persons can have rights or interests in digital assets, which rights or interests can be asserted against third parties, *i.e.*, against persons that are not necessarily contractual parties. This may be particularly relevant in the context of insolvency, where an insolvency representative might assert rights or interests in digital assets on behalf of the insolvency estate against third parties, and where third parties might assert rights or interests in digital assets against the insolvency representative.

Principle 3(2)

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

3.6. As already stated above, these Principles take no position as to whether their rules should be included in a special law on digital assets enacted by a State, should be incorporated into more general laws of a State, already follow from the general law of a State, or are addressed by a combination of these approaches. However, Principles law (as defined in Principle 2(3)) takes precedence over other law (as defined in Principle 2(4)) (see also Commentary 2.18 to 2.22, especially Commentary 2.19). This may be achieved in a State as a result of generally applicable rules that grant precedence to specific laws over general laws, or to later laws over earlier laws. A State may need to specify the laws and sections or articles in other laws that are repealed or superseded.

3.7. It is possible that a State has, or decides to enact, a law that is even more specific than the Principles, such as a law that relates to a particular type of linked asset (see Principle 4). In that situation, the State should ensure that, as far as possible, Principles law in relation to that type of digital asset is consistent with the specific law. For example, a State might want to adopt a slightly different innocent acquisition rule for that type of digital asset (see Commentary 8.7), or it might want to ensure that the secured transactions rules specific to that category of asset apply as appropriate (see Commentary 14.4). To the extent that any conflict remained, the specific law would have precedence over Principles law. An example of such a specific law is the UNCITRAL Model Law on Electronic Transferable Records, which gives functionally equivalent legal effect to electronic equivalents of transferable paper documents and instruments. Such an electronic equivalent could be in the form of a digital asset as defined in Principle 2(2) (see Commentary 4.22 for an example). In a State where the UNCITRAL Model Law on Electronic Transferable Records has been implemented, that law, and the law of that State governing the relevant functional paper equivalent, would have precedence over Principles law in the event of a conflict. However, as mentioned earlier, it is recommended that a State should take steps to avoid inconsistency wherever possible.

Principle 3(3)

3.8. Principle 3(3) makes it explicit that other law (as defined in Principle 2(4)), continues to apply to digital assets. For this purpose, Principle 3(3) lists several examples of issues of property law, but also of contract law, that may continue to be addressed by a State's other law, because these Principles do not cover those issues, nor do they intend to change or derogate from that other law. The list is not intended to be exhaustive or limitative. It is reiterated that, first, these Principles cover only private law issues relating to digital assets, so that they do not cover rules that are to be enforced by public authorities which in many jurisdictions would be called 'regulation' or 'regulatory law'. Secondly, these Principles cover only a specific area of private law, and there are many issues of private law which are not addressed by the Principles. These issues concern, for instance, rules of private law relating to intellectual property or consumer protection. As a matter of principle, these areas of law are not addressed by these

Principles, and national intellectual property and consumer protection laws therefore remain unaffected by them. Finally, as mentioned above, there are several issues of property and contract law that these Principles do not cover, important examples of which are listed in Principle 3(3). Strictly speaking, 'Except as displaced by these Principles' is redundant, because 'other law' (as defined), is, by definition, law that is not covered by these Principles. It is for the avoidance of any doubt that Principle 3(3) says that 'except as displaced by these Principles', other law continues to apply. It is not intended to mean that a specific State law continues to apply only to the extent that these Principles (as contrasted with Principles law) explicitly displace such State law. Although Principle 2(5) defines 'transfer' (as used in these Principles) as including the grant of a security right in favour of a secured creditor, the list in Principle 3(3) refers separately to transfers and security rights. This is for clarity of exposition, and because Principle 3(3) lists matters to which other law applies.

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

3.10. Second, Principles 3(3)(b) and 3(3)(c) concern dynamic situations of acquisition and disposition of a digital asset from the perspective of the transferor and security right provider respectively. If the question arises whether a person has validly transferred a proprietary right, or validly created a security right, in a digital asset, Principles 3(3)(b) and 3(3)(c) make it clear that the requirements for a (valid) transfer or creation of a security right continue to be, as a matter of principle, a matter of other law. However, these Principles do provide some specific rules regarding the transfer of, and third-party effectiveness of a security right in, a digital asset. For example, Principle 15 provides that control (as defined in Principle 6) must be an available method of making a security right in a digital asset

effective against third parties, but other law may provide for other means of achieving effectiveness. Moreover, Principle 8 provides that an innocent acquirer takes free from conflicting proprietary rights and Principle 12 provides similar protection to a client for whom a custodian maintains a digital asset. Whenever it is unclear whether existing rules or standards of general application apply to digital assets, and whenever Principles law derogates from other law, it is recommended that State law make this explicit.

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

3.12. As explained above, Principles 3(3)(d) and 3(3)(e) concern, respectively, the (contractual) relationships between a transferor and a transferee, and between a grantor of a security right and the relevant secured creditor. These provisions thus concern *inter se* relationships, *i.e.*, relationships between (contracting) parties. Principles 3(3)(f) and 3(3)(g), on the other hand, concern *erga omnes* relationships, *i.e.*, the relationships with third parties. Pursuant to Principles 3(3)(f) and 3(3)(g), whether a transfer and a security right, respectively, can be asserted against third parties, continues to be, as a matter of principle, a matter of other law. In some jurisdictions, the 'assertability' of a right or interest against third parties follows from the concept of 'effectiveness'. Principles 3(3)(f) and 3(3)(g) provide that, whatever the doctrinal context, the requirements for such effectiveness or assertability continue to be, as a matter of principle, a matter of other law, except where the Principles provide other rules (see Commentary 3.10 and Principle 15).

Principle 4

Linked assets

The digital assets to which these Principles apply include a digital asset linked to another asset. The other asset may be tangible or intangible (including another digital asset). Other law applies to determine the existence of, requirements for, and legal effect of any link between the digital asset and the other asset, including the effect of a transfer of the digital asset on the other asset.

Commentary

4.1. As provided in Principle 4, a digital asset may be linked to another asset or assets. Principles law takes a neutral stance as to whether this link is sufficiently established and what, if any, the legal effect of the link may be. These matters are instead left to the other law of the State, including its regulatory law, to determine. The operation of the link may depend on other law already in force in the State or on new rules specially developed for linked assets. Consequently, the link between the digital asset and the other asset may operate in a variety of different ways depending on the other law applicable to it.

4.2. One common reason for linking a digital asset to another asset is to enable transactions with the other asset to be effected by a transfer of the digital asset. The intention in creating the link may be to enable the holder of the digital asset to alter a person's rights in relation to the other asset or in relation to a person who issued it. The intention may be that a transfer of the digital asset should have the effect of transferring rights in the other asset.

4.3. The 'other asset' referred to in Principle 4 may be tangible or intangible, and it may be another digital asset or one created under other law, such as a share or bond. The other asset is one which exists contemporaneously with, but separately from, the digital asset. It does not include a 'resulting digital asset', within the meaning of

Principle 6(2), which only comes into existence to give effect to some change in the control of an original digital asset.

Existence and effect of the link

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

4.5. Whether the link is proved to exist is primarily a question of fact. Its existence depends on all the circumstances of the case and the intentions of the parties who created the digital asset. The link may be apparent from the coding of the digital asset or from any related system protocols applying to it. It may also be apparent from any published documentation relating to the digital asset or the other asset, such as a white paper or the terms of issue applying to them. The other law of the State may also be relevant to the existence of the link. The other law (including its regulatory law) may define minimum legal standards for recognising that the link exists. A link which failed to satisfy those standards would be ineffective whatever the intentions of the parties who created the digital asset might have been.

4.6. Even where the factual existence of the link between the digital and the other asset is satisfactorily established, its legal effect depends on other law. 'Legal effect' is to be understood broadly. It includes, most importantly, the effect of any transaction with the digital asset on the parties' rights in relation to the other asset, and the effect of those transactions in insolvency. One consequence of giving legal effect to the link may be that rights in the digital asset and the other asset are transferred synchronously with each other. It may also enable a change in any contractual rights between the holder of the digital asset and the holder of the other asset.

4.7. Consistently with the primacy of other law under this Principle, the parties who issue or transact with the digital asset cannot confer any greater legal effect on the link than the other law of the State would allow. It may not be sufficient, for example, simply for them to provide by a contract between them that a transfer of the

digital asset will necessarily transfer proprietary rights in the other asset. The other law of the State would need to permit or provide for this effect. The contractual agreement may only apply between the parties to it.

Comparison with registry systems

4.8. Transactions with linked digital assets do not always have the same legal effect as transactions with conventional assets, such as securities recorded in a legally constituted registry system. A change in the recorded holding of a digital asset is legally neutral in relation to the other asset unless other law confers a legal effect on the link. Where the other law does so provide, the consequence may be that a transfer of proprietary rights in the digital asset and the other asset would be synchronised.

4.9. With a conventional securities registry, a transfer recorded in the registry has the legal effect of transferring the proprietary interest in the debt or equity securities that it relates to. The reason is that other law, typically legislation, confers legal effect on the registry system. Similarly, it would be open to the other law of a State to provide that a recorded transfer of a digital asset had the effect of transferring the proprietary interest in the other asset, such as a share, that it was linked to. The reason would be that the other law defined the link in such a way that the transfer of digital asset was directly constitutive of the parties' proprietary interests in the other asset.

Form of other law

4.10. The legal effect may be determined by existing rules of other law, or a State may provide for it in special rules developed for linked assets. Other law may recognise the existence of the link without also recognising that a disposition of the digital asset has any legal effect at all on the parties' rights in relation to the other asset. A separate legal act may be required to change the parties' rights to the other asset. Thus, the legal effect of holding and transferring linked assets depends on a combination of these Principles and any rules of other law relevant to the other asset.

Innocent acquisition

4.11. It would be open to the other law of a State to provide that the benefit of any innocent acquisition rule applied to a digital asset in accordance with Principle 8 should also apply to the other asset linked to it. Consistently with the primacy of other law, however, the simple proof of the link between the digital asset and the other asset would not necessarily mean that the holder of the other asset took the benefit of the innocent acquisition rule. The other law of the State would need to provide for this result. See Commentary 4.29 to 4.32: Illustration 8.

4.12. As illustrations of the different legal effects of a link between the digital asset and the other asset, eight examples follow.

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

4.14. For example, a system may be established for trading quantities of tokenised gold. An investor may hold a digital token which evidences a proprietary right in a fractional share of specifically identified gold. Whether a sale and transfer of the token passes the seller's proprietary right in the gold depends on the rules that apply to the gold in the relevant State's other law. In some legal systems, the other law may treat the parties' dealings with the digital token as the outward expression of their intention to transfer the proprietary right in the gold. The proprietary right in the gold would pass to the buyer of the token. The State would not need to enact any new rule of other law for this to happen (as an aside, it should be noted that even if the other law of the State permitted this effect, it would not necessarily preclude the parties from transacting directly with the gold separately from the digital token. If so, the effect would be that the proprietary interests in the gold and the token would become desynchronised.)

4.15. In other States, other law may provide that the seller must deliver the gold to the buyer in order to pass the proprietary right in it. In that case, a sale and transfer of the token would not pass the proprietary right in the gold. A new rule of other law might need to be enacted to synchronise the transfer of the proprietary rights in the two assets.

4.16. ***Illustration 2.*** One digital asset may be linked to another digital asset and the legal link between them would depend on the effect of any legal relations between the holders of the two assets.

4.17. For example, an issuer may create a digital asset which is a 'wrapped' version of another digital asset on a different protocol. Like the 'stable coin' in Illustration 6, only one 'wrapped' digital asset would be created for every other digital asset on the other protocol. The white paper may provide that the holder of the wrapped digital asset is entitled to redeem the other digital asset. In return, the holder's wrapped digital asset would be 'burned'. The effect of this 1:1 relationship is that the value of the wrapped digital asset should correspond to the value of the other digital asset. When the wrapped digital asset is transferred, the transferee should receive the same value as if the other digital asset had been transferred between them. The rights of the holder of the wrapped asset in relation to the other asset would depend on the legal effect of the link between them. The terms of a contract between the issuer and holder of the wrapped digital asset would determine if the holder had a right to regain control of the other digital asset and have the wrapped asset 'burned' at that point. It should be noted that in Illustrations 2, 6 and 7, the word 'issuer' is not used with the limited meaning set out in Principle 5(2)(f).

4.18. ***Illustration 3.*** The rules of other law already in force may govern all proprietary aspects of an asset linked to a digital asset, regardless of the representations and intention of the parties dealing in these assets.

4.19. For example, a person (Alpha) may create a non-fungible digital asset (A-NFT) that is recorded in a blockchain ledger maintained and operated through a public, permissionless, distributed network. Alpha may make written and verbal representations that she intends for A-NFT to embody all her copyrights relative to a musical work of her creation. Moreover, Alpha may enter into a transaction with another person (Beta) in which they agree that, by transferring the A-NFT, Alpha assigns her copyrights to Beta and that Beta may subsequently re-assign these copyrights to others by transferring to them the A-NFT. Regardless of Alpha's intention to tokenise her copyrights, the applicable copyright law will determine whether the link between the A-NFT and her copyrights has any legal effect.

Analogously, the applicable copyright law will determine whether transferring the A-NFT constitutes a valid assignment of the copyrights in question, as well as whether Beta can subsequently re-assign these copyrights by re-transferring the A-NFT.

4.20. ***Illustrations 4 and 5.*** A State may choose to enact special legislation to make the link between the token and the other asset legally effective.

4.21. For example, a company may raise finance from investors by issuing debt securities on a blockchain ledger. Each investor holds a transferable digital token representing their claim against the company. The terms of issue purport to give the investor a right to payment by the company who has issued the debt securities. When the token is transferred on the ledger, the transferee acquires the right against the company. The company which issued the debt security gets an effective discharge if it pays the current holder of the token. Special legislation may be needed to effect this result if it cannot be achieved, for example, by the State's existing other law of contract, assignment, novation, or securities transfer.

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

4.23. ***Illustration 6.*** The precise legal effect of any link between the digital asset and another asset may depend as much on ascertaining the parties' intentions from any system coding, protocols, and documentation as it does from the operation of the other law. Thus, the terms of a white paper accompanying the issue of a digital asset may be relevant to inferring the nature and value of the legal right, if

any, that the holder of the digital asset was intended to have in relation to the other asset.

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

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

4.26. ***Illustration 7.*** Digital assets may be used to create transferable portions of value derived from other assets which exist off the blockchain. Even where the link between the digital assets and the other assets is clear, the precise effect of the holders' rights will be determined by the other law of the State. The parties' intention to link the assets cannot override the other law that applies to those assets.

4.27. For example, an issuer may sell digital assets that purport to give the holder a claim in relation to real estate. The assets are transferable on a blockchain ledger. On closer analysis, most tokenised real estate actually involves the establishment of a company to which ownership of the real estate is transferred. The shares in the company are then 'tokenised' and made transferable on the ledger.

The transfer of the token may not be sufficient in law to transfer the shares in the company or any proprietary interest in the real estate. These may be questions for the system of other law where the company is registered, or the real estate is located. The relevance of the digital asset is to illustrate (i) the 'chain' of legal relations between the holder and the shares and the real estate, and (ii) steps that may need to be taken by the acquirer of the token to update a company register; or update a register of real estate.

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

4.29. ***Illustration 8.*** The other law of a State may recognise a good faith acquisition rule in relation to the other asset linked to the digital asset. The effect may be that both the digital asset and the other asset would benefit from a good faith acquisition rule.

4.30. For example, as in Commentary 4.13 to 4.15, a system may be established for trading quantities of tokenised gold and an investor may hold a digital token which evidences a proprietary right in a fractional share of specifically identified gold. A hacker may unlawfully obtain control of the token and transfer it by sale to an innocent buyer. Under Principle 8, the buyer would acquire a proprietary interest in the token which was free from the claims of the original investor who once held the token. It would be, however, for the other law of the State to determine whether the innocent buyer would also acquire a proprietary right in the 'linked' share of the gold and also take it free of the original investor's claims.

4.31. The other law of a State may provide similar consequences for a linked asset subject to a security right. A security right may be granted in a digital token that purports to evidence a proprietary right in a fractional share of gold. Whether the security right extends to the gold is a matter of other law. Developing the example in Commentary 4.20 to 4.22, the other law may, for instance, treat the digital token evidencing a proprietary right to gold as a document of title, in which case a security right in the token would extend to the gold. Any such

system would have to consider carefully how to address rights in the linked asset so that all rights 'reside' in the token.

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

SECTION II: PRIVATE INTERNATIONAL LAW

Principle 5

Applicable law

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

(a) the domestic law of the State expressly specified in the digital asset, and those Principles (if any) expressly specified in the digital asset; or, failing that,

(b) the domestic law of the State expressly specified in the system on which the digital asset is recorded, and those Principles (if any) expressly specified in the system on which the digital asset is recorded; or, failing that,

(c) in relation to a digital asset of which there is an issuer, including digital assets of the same description of which there is an issuer, the domestic law of the State where the issuer has its statutory seat, provided that its statutory seat is readily ascertainable by the public; or

(d) if none of the above sub-paragraphs applies:

OPTION A:

(i) those aspects or provisions of the law of the forum State as specified by that State;

(ii) to the extent not addressed by sub-paragraph (d)(i), those Principles as specified by the forum State;

(iii) to the extent not addressed by sub-paragraphs (d)(i) or (d)(ii), the law

applicable by virtue of the rules of private international law of the forum State.

OPTION B:

(i) those Principles as specified by the forum State;

(ii) to the extent not addressed by sub-paragraph (d)(i), the law applicable by virtue of the rules of private international law of the forum State.

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

(a) proprietary issues in respect of digital assets, and in particular their acquisition and disposition, are always a matter of law;

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

(c) by transferring, acquiring, or otherwise dealing with a digital asset a person consents to the law applicable under sub-paragraph (1)(a), (1)(b) or (1)(c);

(d) the law applicable under paragraph (1) applies to all digital assets of the same description;

(e) if, after a digital asset is first issued or created, the applicable law changes by operation of sub-paragraph (1)(a), (1)(b) or (1)(c), proprietary rights in the digital asset

that have been established before that change are not affected by it;

(f) the 'issuer' referred to in sub-paragraph (1)(c) means a legal person:

(i) who put the digital asset, or digital assets of the same description, in the stream of commerce for value; and

(ii) who, in a way that is readily ascertainable by the public,

(A) identifies itself as a named person;

(B) identifies its statutory seat; and

(C) identifies itself as the person who put the digital asset, or digital assets of the same description, into the stream of commerce for value.

(3) The law applicable to the issues addressed in Principles 10 to 13, including whether an agreement is a custody agreement, is the domestic law of the State expressly specified in that agreement as the law that governs the agreement, or if the agreement expressly provides that another law is applicable to all such issues, that other law.

(4) Paragraphs (1) and (2) are subject to paragraph (3).

(5) Other law applies to determine:

(a) the law applicable to the third-party effectiveness of a security right in a digital asset made effective against third parties by a method other than control;

(b) the law applicable to determine the priority between conflicting security rights

made effective against third parties by a method other than control.

(6) Notwithstanding the opening of an insolvency-related proceeding and subject to paragraph (7), the law applicable in accordance with this Principle governs all proprietary issues in respect of digital assets with regard to any event that has occurred before the opening of that insolvency-related proceeding.

(7) Paragraph (6) does not affect the application of any substantive or procedural rule of law applicable by virtue of an insolvency-related 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;

(c) the enforcement of rights to an asset that is under the control or supervision of the insolvency representative.

Commentary

General

5.1. It is recognised that a conflict-of-laws rule will always be imperfect. The aim of Principle 5 is therefore to improve the clarity and legal certainty surrounding the issue of conflict-of-laws to the greatest possible extent.

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

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

5.4. Principle 5 recognises that the usual connecting factors for choice-of-law rules (*e.g.*, the location of persons, offices, activity, or assets) usually have no useful role to play in the context of the law applicable to proprietary issues relating to digital assets. Indeed, adoption of such factors would be incoherent and futile (except in the limited case where there is an identified issuer, see Principle 5(1)(c)) because digital assets are intangibles that have no physical situs. Instead, the approach of this Principle is to provide an incentive for those who create new digital assets or govern existing systems for digital assets to specify the applicable law in or in association with the digital asset itself or the relevant system. This approach would accommodate the special characteristics of digital assets and the proprietary questions concerning digital assets that may arise.

Principles 5(1)(a) and 5(1)(b)

5.5. Principle 5(1) provides a 'waterfall' of factors for the determination of the applicable law. Under Principle 5(1)(a), the applicable law is the domestic law of the State specified in the digital asset itself, together with any of the Principles that are specified. If Principle 5(1)(a) does not apply, the applicable law is that of the State specified in the system in which the digital asset is recorded, together with any of the Principles that are specified (Principle 5(1)(b)) (for a discussion of the notion of 'system' see Commentary 5.6). The choice-of-law rules in Principles 5(1)(a) and 5(1)(b) are based on party autonomy, for the reasons given in Commentary 5.4 and also because Principle 5(2)(c) treats every person dealing with a digital asset, and who could be affected by a determination of a proprietary issue, as consenting to the choice-of-law rules in Principle 5(1) (see also Commentary 5.16). Such persons will know about the specification of the applicable law, since it will be in records readily available for review by such persons (see Principle 5(2)(b) and Commentary 5.16). Moreover, although many digital assets, or systems, currently do not include a specification of applicable law, the rules in Principles 5(1)(a) and 5(1)(b) provide an incentive for such a specification to be included. This reliance on party autonomy is consistent with Article 3 of the Hague Conference Principles on Choice of Law in International

Commercial Contracts ('Hague Conference Principles'). It would also be possible for a digital asset, or a system, to specify that these UNIDROIT Principles or some of them (supplemented where necessary by the specified domestic law) would be the law applicable to proprietary issues.

5.6. The notion of 'system' in Principle 5(1)(b) should be understood as technology neutral and construed both broadly and functionally. It includes any type of protocol, platform, application, transfer arrangement, and network in so far as it has the capabilities necessary to record digital assets. It should be noted that networks are generally built in layers (*e.g.*, physical layer, data link layer, network layer, transport layer, session layer, presentation layer, and application layer), so that a digital asset can be recorded in an application that operates and relies on a platform which, in turn, operates and relies on a protocol. It is possible that a different applicable law is specified for two or more layers. To address the ensuing uncertainty, a State might consider adopting a specific rule to determine which law applies in these circumstances. An example of such a rule could be that the applicable law specified by the layer closer to the digital asset prevails. The question of which layer is closer is a matter of fact which will need to be determined by the competent court. The uncertainty identified in this paragraph would, however, not arise if the applicable law were specified in the digital asset (Principle 5(1)(a)).

5.7. As stated above, Principle 5(1) provides a 'waterfall' of connecting factors for the determination of the applicable law. Under Principle 5(1)(a), the applicable law is the domestic law of the State specified in the digital asset itself. The digital asset can also specify all or some of the Principles as the applicable law: in that case, these would take precedence over the specified domestic law (see Principle 3(2)). However, even if all the Principles were specified, a domestic law would also need to be specified as this would apply to issues which are, under the Principles, a matter of other law. If Principle 5(1)(a) does not apply, the applicable law is the domestic law of the State specified in the system on which the digital asset is recorded, plus all or some of the Principles if specified, as discussed above. If a choice of law has been made neither in the digital asset itself, nor in the system on which it is recorded, the law of the issuer's State applies as per Principle 5(1)(c). The law so determined, *i.e.*, the issuer's law, governs not only the specific digital asset that may be the object of a

concrete case, but all digital assets that are 'of the same description' (see Principle 5(2)(d)). 'Of the same description' means, in these Principles, digital assets that are treated by market participants as fungible. See also Commentary 11.6.

Principle 5(1)(c)

5.8. Principle 5(1)(c), *i.e.*, the third step down the waterfall provided by Principle 5, is of limited scope. The scope is limited, first, because not all digital assets will have an issuer (as defined in Principle 5(2)(f), see Commentary 5.10). In all those instances, this rule will not apply, and the applicable law is to be determined under Principle 5(1)(d). See, however, for examples of digital assets that are typically issued, Commentary 4.23 to 4.28.

5.9. Second, the connecting factor of the issuer is qualified in multiple ways. Importantly, Principle 5(1)(c) refers to the State where the issuer has its statutory seat. If one must determine an issuer's location, its statutory seat is the connecting factor that gives most certainty as it is most easily identifiable by third parties. Other possible connecting factors, such as the place of 'central administration', the 'principal place of business', or the 'centre of main interest' cannot be identified with the same level of certainty and would therefore introduce an unwarranted measure of uncertainty. Under Principle 5(1)(c), the issuer's statutory seat must be 'readily ascertainable by the public'. If, for instance, the issuer does not have a statutory seat because it is an informal partnership, there would be no statutory seat that is 'readily ascertainable by the public' as per Principle 5(1)(c). Also, if it were unclear which issuer issued a specific digital asset because the digital asset is issued by different persons or in different layers, the statutory seat of the issuer of this digital asset would not be readily ascertainable by the public. In all those instances, Principle 5(1)(c) will not apply and the applicable law is to be determined under Principle 5(1)(d).

5.10. Third, 'issuer' is defined in Principle 5(2)(f), and a person must meet no less than five cumulative criteria to qualify as an issuer. First, for a person to qualify as an issuer, it must be a legal person. Natural persons are therefore excluded from qualifying as an 'issuer' under these Principles. This criterion could already be inferred from Principle 5(1)(c), where reference is made to the issuer's statutory seat,

which logically can only refer to a legal person. Also, from Principle 5(1)(c), read in conjunction with the chapeau of Principle 5(2)(f), it must be inferred that if the relevant issuer does not qualify as a legal person (for instance, because an informal partnership is not recognised as a legal person under the applicable law), Principle 5(1)(c) does not apply. In all these instances, the applicable law must be determined under Principle 5(1)(d). Second, the issuer must have put the digital asset, or digital assets of the same description, in the stream of commerce for value as per Principle 5(2)(f)(i). This criterion is meant to exclude instances in which a digital asset is created by a person who has no further commercial interest in it. On the concept of 'the same description', see Commentary 5.17 and Commentary 11.6). Third, for a person to qualify as an issuer, that person must have identified itself as a named person in a way that is readily ascertainable by the public as per Principle 5(2)(f)(ii)(A). This means that the name of the issuer must be easily identifiable by third parties. Fourth, the issuer must have identified its statutory seat in a way that is readily ascertainable by the public as per Principle 5(2)(f)(ii)(B). This criterion seems self-explanatory. Finally, the issuer must have identified itself, in a way that is readily ascertainable by the public, as the person who put the digital asset, or digital assets of the same description, into the stream of commerce for value as per Principle 5(2)(f)(ii)(C). This means that not only must the issuer have put the digital asset in the stream of commerce for value as a matter of fact (as per Principle 5(2)(f)(i)), it also must have identified itself as such (in a way that is easily identifiable by third parties). Again, should a person not comply with any (or all) of the criteria for qualification as issuer under this Principle 5(2)(f), the applicable law must be determined under Principle 5(1)(d).

Principle 5(1)(d)

5.11. At the bottom of the 'waterfall', in the absence of a specification made in the digital asset or the system as contemplated by Principle 5(1)(a) and Principle 5(1)(b), and if Principle 5(1)(c) does not apply, Principle 5(1)(d) provides a State with a considerable degree of freedom to choose the appropriate rules for a forum sitting in that State. An overarching consideration is the fact that in many cases the digital asset may have no significant connection with any State. It is not feasible to specify in Principle 5(1)(d) a definitive, 'one size fits all'

approach to be applied by the forum to proprietary questions in respect of a digital asset. Principle 5(1)(d) therefore provides for two options (Option A and Option B): each includes the application of some or all of the Principles (as specified by the forum State) to such questions. Because these Principles are generally accepted on an international level as a neutral and balanced set of rules, their application at the bottom of the waterfall is appropriate (see Article 3 of the Hague Conference Principles that 'allows the parties to choose not only the law of a State but also 'rules of law', emanating from non-State sources.'). It is important to emphasise that the Principles applicable under each option are only those specified by the forum State.

5.12. Within each option in Principle 5(1)(d), there is a 'waterfall' set out in sub-paragraphs, based on specifications made by a State when adopting Principle 5.

Option A

5.13. Option A is suitable if a State decides that it is appropriate for the forum sitting in that State to apply some aspects of its own domestic law in respect of proprietary issues in relation to a digital asset. This might be the case, for example, if the State has adopted laws that deal specifically with proprietary issues relating to digital assets. One example of this would be where the State has already adopted some aspects of these Principles as part of its domestic law. These aspects of domestic law specified by the forum State form the first part of the waterfall (Principle 5(1)(d)(i) of Option A). The second part of the waterfall (Principle 5(1)(d)(ii) of Option A) relates to matters not addressed by Principle 5(1)(d)(i) of Option A, and is comprised of either the (entire) Principles, or some Principles or some aspects of the Principles, according to the choice, and consequent specification, of the forum State. The third part of the waterfall (Principle 5(1)(d)(iii) of Option A), which applies to the extent not addressed by other clauses, requires the forum to apply the law otherwise applicable under its private international law rules.

Option B

5.14. Option B consists of the second and third parts of the waterfall set out in Option A. It therefore is suitable for a State which

determines that proprietary issues relating to digital assets should be determined only by the Principles or some portions thereof, without any reference to substantive domestic laws. This might be the case, for example, if the State has not adopted laws that deal specifically with proprietary issues relating to digital assets. Again, the applicable Principles are those specified by the forum State. The third part of the waterfall applies as set out in Commentary 5.13.

5.15. By making reference to these Principles, Principle 5(1)(d) provides an innovative means of permitting a forum to adopt the Principles for persons and matters subject to its jurisdiction where none of Principles 5(1)(a), 5(1)(b) or 5(1)(c) applies. The adoption of Principle 5 would accommodate the wish of a forum to adopt the Principles in such situations. In particular, the forum would apply the Principles even where the substantive law of a forum State itself would otherwise apply, without the potential delay and complexity in making substantial revisions of otherwise applicable local private law. Indeed, a forum State might choose this approach either as its primary means of adopting the Principles or as an interim approach, pending their full adoption. Of course, if the relevant digital asset or system specified the substantive law of the forum State (which would thereby apply under Principles 5(1)(a) or 5(1)(b)) it is reasonable to assume that the forum State would have adopted acceptable substantive rules such as those exemplified by these Principles. Principle 5 leaves considerable flexibility for a State to craft choice-of-law rules that conform to its policy judgments and are compatible with its domestic law.

Principle 5(2)

5.16. Paragraph (2) provides additional guidance on the interpretation and application of Principle 5(1). Principle 5(2)(a) confirms that proprietary issues are subject to law regardless of whether (i) the participants in the relevant network refute the application of any law and exclusively want to rely on code, and (ii) 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. Principle 5(2)(b) makes it clear that a specification of applicable law in a digital asset, or in a system, can be determined by looking at records (in the sense of information

recorded electronically or by other means) attached to or associated with the digital asset, system, but only if such records are readily available for those dealing with the asset. Persons dealing with the asset, who will be able to view these records, are treated, by virtue of their dealing, as having consented to the specified applicable law: this is the effect of Principle 5(2)(c).

5.17. The effect of Principles 5(2)(d) and 5(2)(e) is that the specified applicable law applies to all digital assets of the same description from the time the digital asset is created or issued, but if the applicable law changes from a later time, pre-existing rights in the digital asset are not affected. It is particularly important that all digital assets of the same description be governed by the same applicable law. Changes in the applicable law should be avoided if at all possible. If such changes were to occur, transitional provisions that ensure that the same law applies to all such digital assets at all times would be essential. Principle 5(2)(f) is discussed in Commentary 5.10.

Principles 5(3) and 5(4)

5.18. Principles 5(3) and 5(4) make it clear that Principle 5(1) does not determine the law applicable to the relationship between a custodian and its client. This question is determined by the choice-of-law rule in Principle 5(3), namely, that the applicable law is the law expressly stated in the custody agreement as governing that agreement or, if different, the law expressly stated as governing the issues addressed in Principles 10 to 13. This rule would typically result in the application of a single law to those matters. It is appropriate for one law to apply to the custody relationship, rather than different laws, as might be specified in different digital assets or different systems as contemplated by Principles 5(1)(a) and 5(1)(b).

5.19. The specific conflict of laws rule provided in Principle 5(3) determines the applicable law in the relationship between a custodian and its client, but it is limited in scope. This rule only concerns the issues addressed in Principles 10 to 13, including whether the agreement is a custody agreement. Principle 13 addresses issues arising if a custodian enters into an insolvency-related proceeding. As is shown by Principles 5(6) and 5(7), the conflict of laws rule in Principle 5(3) applies to contractual and proprietary issues addressed

in Principles 10 to 13, but insolvency law issues will be governed by the applicable insolvency law.

5.20. The issues covered by the choice-of-law rule in Principle 5(3) are generally considered to be issues of private law. This rule therefore does not prejudice the application of any rule of regulatory law that may concern the custodian - client relationship. See, for examples of such regulatory rules, Commentary 10.21. Moreover, a custodian may be a regulated entity, and regulatory authorities may wish to restrict a custodian's choice of law for the custody agreement or for the issues covered by Principles 10 to 13. Principle 5(3) does not set aside any such rule of regulatory law restricting the custodian's choice of law.

5.21. By excluding the custody relationship from the application of Principles 5(1) and 5(2), it is not suggested that those Principles do not apply to proprietary issues such as where a custodian acquires, or disposes of, a digital asset.

Principle 5(5)

5.22. Principle 5(5) recognises that the approach taken in Principle 5(1) would be inappropriate to determine the law governing a registration system for security rights, which must be based on objective indicia (such as the location of the grantor) that could be determined by a third-party searcher of the registry.

5.23. For the reason given in Commentary 5.22, Principle 5(5) provides that other law (in this case, the conflicts of law rules contained in other law) determines the law applicable to third-party effectiveness of a security right in a digital asset made effective against third parties by a method other than control. In addition, because the same law also needs to govern priority between two or more such security rights, Principle 5(5) provides that other law determines the law applicable to determine priority between such conflicting security rights. If one conflicting security right is made effective against third parties by control (even if it is also made effective against third parties by a method other than control), Principle 5(1) does apply to determine the applicable law. See also Commentary 16.5.

Linked assets

5.24. Where a digital asset is linked, or purports to be linked, to another asset, other law (in this case, the conflicts of law rules contained in other law) determines the law applicable to determine the existence of, requirements for, and legal effect of any link between the digital asset and the other asset. These matters are determined by other law under Principle 4.

Principles 5(6) and 5(7)

5.25. Principle 5(6) makes it clear that in an insolvency-related proceeding Principle 5 should be applied to proprietary questions in respect of a digital asset relating to events occurring before the opening of the insolvency-related proceeding. Principle 5(7) provides the usual exceptions that defer to the applicable insolvency law. These exceptions are discussed in Commentary 19.9 to 19.12. It should be noted that the term 'control' in Principle 5(7)(c) is used in a broad sense, and not as defined in Principle 6 (see Commentary 19.4).

SECTION III: CONTROL AND TRANSFER

Principle 6

Control

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

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

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

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

(iii) the exclusive ability to transfer the abilities in sub-paragraphs (a)(i), (a)(ii) and (a)(iii) to another person; and

(b) the digital asset, or the relevant protocols or system, allows that person to identify itself as having the abilities set out in sub-paragraph (a).

(2) A 'change of control' means a transfer of the abilities in sub-paragraph (1)(a) to another person, and includes the replacement, modification, destruction, cancellation, or elimination of a digital asset, and the resulting and corresponding derivative creation of a new digital asset (a 'resulting digital asset') which is subject to the control of another person.

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

(a) the digital asset, or the relevant protocol or system, limits the use of, or is

programmed to make changes to, the digital asset, including change or loss of control of the digital asset; or

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

Commentary

General

6.1. The concept of 'control' is of great importance in these Principles. Principle 6 contains a detailed definition of control of a digital asset. Although control is a factual concept that is separate from, and need not accompany, proprietary rights, the existence of 'control' pursuant to the definition in Principle 6 is a requirement for certain legal consequences in these Principles (for example, as a condition precedent to qualification as an innocent acquirer, and for third-party effectiveness and priority of security rights). The exclusive ability requirements in Principle 6(1)(a) (as relaxed in Principle 6(3)) recognise that the ability to exclude is an inherent aspect of proprietary rights.

6.2. The exclusive ability requirements in Principle 6(1)(a) contemplate that 'control' assumes a role that is a functional equivalent to that of 'possession' of movables. However, 'possession' in this context is a purely factual matter and not a legal concept. Moreover, because a digital asset is intangible, this functional equivalence to possession involves only the dominion and power over a digital asset but does not involve the physical situs dimension applicable to possession of movables. Whether 'control', as defined in Principle 6, exists is a matter of fact and does not depend on a legal conclusion. However, as explained below, the presence of control gives rise to legal consequences. The exclusivity criterion of control (including the standards in Principle 6(3) 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.

6.3. Although control assumes a role that is, as a purely factual matter, a functional equivalent to that of 'possession', control as used in these Principles must not be understood to be identical to 'possession' as a legal concept used in certain jurisdictions. In those jurisdictions, possession is a legal concept and a possessor may 'hold' possession of an asset through another person. However, under these Principles control is a factual matter and a person cannot control a digital asset unless the criteria of Principle 6 are met. On the custody of digital assets, see also below and Principle 10.

6.4. 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 and a basis of priority of security rights in a digital asset. States also may choose to adopt the concept of control as an element of third-party effectiveness of proprietary interests more generally. It is important to note that control (as defined in Principle 6) is also an element in the definition of 'digital asset' in Principle 2(2): only an electronic record which is capable of being subject to control is a 'digital asset' and therefore within the scope of the Principles.

6.5. The change of control from one person to another person must be distinguished from a transfer of a digital asset or an interest therein, *i.e.*, a transfer of proprietary rights. See Principle 2(5) (defining 'transfer'). Whether there is a valid transfer of proprietary rights in a digital asset is a matter of other law and is not dealt with in these Principles (see Principle 3(3) and Commentary 2.26). Whilst in many situations a transfer of proprietary rights will be accompanied by a change of control, in some situations it may not. The law of a State, for instance, may provide that under certain circumstances 'ownership' (as defined by the applicable national law) in a digital asset may pass to another person, whilst control stays with the transferor. Vice versa, in some situations, and depending on the applicable other law, a change of control will not result in a transfer of proprietary rights. A custodian (as defined in Principle 10(1)), for instance, may obtain control of a digital asset for a client, but will typically not in that context acquire 'ownership' (as defined by the applicable national law) of that digital asset. This explanation reflects the understanding of control of a digital asset as a functional equivalent of possession.

In an effort to highlight this distinction between changes of control and transfers of proprietary rights, instead of references to, *e.g.*, a 'delivery', a 'delivery of control', or similar references, these Principles refer simply to a 'change of control'. 'Change of control' is defined in Principle 6(2) and two illustrations of change of control are given in Commentary 6.14 to 6.17.

6.6. Control by a person of a digital asset as agent (for example, an employee may have control for their employer), is treated in these Principles as control by the principal, as an implementation of the law of agency. The concept of control is also relevant in the context of the custody of digital assets. As set out in Principle 10, under a custody agreement a service provider is obliged to maintain digital assets for its clients, either by controlling the digital assets itself or by entering into a custody agreement with a sub-custodian whereby the sub-custodian controls the digital assets for the service provider. This is an example of one person (the custodian) having control while proprietary rights are transferred to or remain with another person (the client). A thief of digital assets would be another example of the separation of control and proprietary rights.

'Ability' of a person with control

6.7. In Principle 6 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 Commentary 6.10 to 6.12.

6.8. Principle 6(2) 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 the one 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.

6.9. The requirements in Principle 6(1)(a) (as relaxed in Principle 6(3)), as noted above, reflect the ability to exclude as an inherent attribute of proprietary rights. However, it is possible that a person (other than a person rightfully in control) who has no proprietary rights might acquire these abilities without the consent of the rightful control person, such as by the discovery of relevant private keys through 'hacking', finding, or stealing a device or other record on which the keys are stored. This underscores the distinction between a change in control and a transfer of proprietary rights. Although control is functionally analogous to possession inasmuch as it is a condition for innocent acquisition under Principle 8 and for third-party effectiveness under Principle 15, and a person in control may or may not have proprietary rights in the digital asset, there are important differences.

Exclusivity of abilities

6.10. The exclusive abilities contemplated by Principles 6(1)(a)(i) and 6(1)(a)(iii) assume the existence of a system for digital assets that reliably establishes those abilities and their exclusivity. But the abilities and exclusivity are not negated by the possibility that such a reliable system might be compromised by a wrongful 'hacking' – even if such a wrongful compromise actually occurs. Such a possibility is an inherent, if unfortunate, attribute of any digital asset (as is the improper taking of physical possession of a tangible object from a person in physical possession of the tangible object). As a practical matter, however, past experience indicates that the occurrence of such a hack would be likely to result in a prompt change of control by the wrongdoer. See also Commentary 7.2. Moreover, even if another person were to obtain the relevant abilities without the affirmative consent of the rightful control person, the rightful control person would continue to have control until such time as it no longer has the requisite abilities (*i.e.*, the abilities are lost because control had been transferred to another person). The rightful control person would not lose control merely because the other person obtained those abilities (as by discovering the private key associated with a digital asset) so long as the other person acquiring the abilities had not transferred control. The other person might acquire the abilities innocently and with no intention or reason to transfer control. A person acquiring the abilities wrongfully, however, presumably would not sit idly by

while allowing the rightful control person to maintain the ability to deal with the digital asset. Such a wrongful acquirer presumably would promptly transfer control, as mentioned above. Were the rightful control person to discover that the other person had acquired the abilities, presumably it would either immediately transfer control to protect its interests or would acquiesce in the other person's shared control. It follows that it is unlikely that shared control with another person in the absence of the rightful control person's actual or implicit agreement, consent, or acquiescence would continue beyond a very short period of time.

6.11. Principle 6(3) provides explicit relaxation of the exclusivity requirements imposed by Principle 6(1)(a). Principle 6(3)(a) contemplates situations in which the inherent attributes of a digital asset or the system in which it resides may result in changes, including a change of control, which constitute exceptions to the exclusivity of a control person's abilities. Principle 6(3)(b) recognises that a person who has control may wish to share its abilities with one or more other persons for purposes of convenience, security, or otherwise. For example, in a multi-signature (multi-sig) arrangement, if a person can identify itself under Principle 7(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 at Commentary 6.13. Another example is that of multi-party computation (MPC) in which the private key is split up into several shards, all of which are required to execute a transaction.

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

Shared control

6.13. ***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 Principle 6(1)(a) and can identify itself as provided in Principle 6(1)(b), Investor has control over the digital asset. Although Investor has shared the ability to change control specified in Principle 6(1)(a)(iii) and action by X or Y is a condition for Investor to exercise that ability, Principle 6(3)(b) provides an exception to the exclusivity requirement of Principle 6(1)(a)(iii).

Change of control

6.14. ***Illustration 2: Change of control via PKI.*** A public, permissionless, distributed network (Alpha) supports a virtual machine (Alpha-VM) that enables the creation and use of electronic records (Beta) in its database (Alpha-DB). Alpha implements a public-key cryptography system, whereby every Beta is associated with a public key and can be used only by a person who sends the appropriate instructions to the Alpha-VM validated by the corresponding private key. Alpha and the Alpha-VM support two uses for Betas. First, a person can actuate a Beta to record a small image file into the Alpha-DB permanently; each Beta can be actuated only once. Second, a person can change the public key with which a Beta is associated; after a Beta has been associated with a new public key, its corresponding private key is required to use that Beta.

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

6.16. ***Illustration 3: Change of control via OTP-Device.*** A private, permissioned, distributed network (Gamma) supports a

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

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

Principle 7

Identification of a person in control of a digital asset

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

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

(b) if that person demonstrates that it has the abilities specified in Principles 6(1)(a)(i) and 6(1)(a)(iii), those abilities are presumed to be exclusive.

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

Commentary

7.1. 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 Principle 7. If the control of a person is challenged, it would be impossible for the putative control person to prove with certainty a negative – that no person other than one permitted by the definition has the relevant abilities. Principle 7(1)(a) makes it clear (although it would be implicit in any event) that a person asserting that it has control of a digital asset establishes a presumption 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. Principle 7(1)(b) dictates a similar result in relation to exclusivity of abilities through the operation of a presumption, the operation of which would be governed by the applicable domestic procedural law. Of course, a person who

previously (rightfully) had control may demonstrate under applicable domestic law that it has a better proprietary interest than the person who currently has control by proving that the change of control was wrongful. The presumption can be overcome by sufficient proof under the State's procedural rules.

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

Principle 8

Innocent acquisition

(1) In order to qualify as an innocent acquirer, a transferee must:

(a) obtain control of a digital asset; and

(b) comply with requirements equivalent to those found in the relevant good faith acquisition and take-free rules as specified by the relevant State.

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

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

(4) An innocent acquirer can acquire a proprietary right in a digital asset even if control of that digital asset is changed by a transferor who is acting wrongfully and has no proprietary right in the digital asset.

(5) If these Principles are applied pursuant to Principle 5(1), in addition to the requirement in sub-paragraph (1)(a), the following requirements for a transferee to be an innocent acquirer apply with respect to a digital asset:

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

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

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

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

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

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

(6) Except as provided in Principle 9, if a transferee is not an innocent acquirer under paragraph (1) or, if applicable, paragraph (5), other law applies to determine the rights and liabilities, if any, of that transferee.

Commentary

General

8.1. As is made clear in Principle 9 and its Commentary, the basic rule of *nemo dat quod non habet* (one cannot give what one does not have) applies to digital assets. However, this is subject to the innocent acquisition rule set out in Principle 8, which is an exception to the basic *nemo dat* rule. As set out in Principles 8(2) and 8(3), an innocent acquirer takes free of conflicting proprietary rights, and no rights based on a proprietary claim can be asserted against an innocent acquirer.

8.2. The rights conferred on innocent acquirers in accordance with Principles 8(2) and 8(3) mean that digital assets will have attributes similar to those of negotiability under rules applicable to negotiable instruments, negotiable documents of title, and negotiable certificated securities in many common law and civil law jurisdictions.

8.3. It is recognised that the result of an innocent acquisition rule is that, in some circumstances, a person with a proprietary claim, who is the victim of wrongful activity, will not be able to assert that claim successfully against the innocent acquirer. The victim would have a claim against the wrongful actor, but that is unlikely to be effective. The innocent acquisition rule represents a policy balance, in this situation, in favour of an innocent acquirer for the reasons set out in Commentary 8.4 and 8.5.

8.4. Digital assets are often traded on a distributed ledger system or other electronic networks that permit near instantaneous transactions. The fluidity of the market allows for transactions that recognise the full value of these assets and transactions. This fluidity, and the fact that many transferors are pseudonymous and often based in different jurisdictions, makes investigations as to whether there are any conflicting proprietary rights in the asset being acquired highly impractical. A person who has a proprietary right in a digital asset is therefore in a better position than a transferee to protect itself from wrongful activity by taking steps to safeguard its proprietary rights. The availability of an innocent acquisition rule would facilitate the types of transactions referred to above and would contribute to legal certainty and efficient markets. In the absence of an innocent acquisition rule, the risk of third-party proprietary claims to a digital asset would be likely to be factored into, and reduce, the amount that a prudent buyer would be willing to pay for the digital asset or the value a secured creditor would assign to the digital asset as an encumbered asset. Moreover, the legal certainty provided by an innocent acquisition rule also benefits custodians of digital assets and their clients (see also Principle 12 and its Commentary). The availability of an innocent acquisition rule will reduce friction in transactions and reduce costs for all involved. The availability of innocent acquirer status in other areas, such as negotiable instruments and securities, has proved effective and safe for the operation of those

markets. Digital assets are playing an important role in the current economy and are expected to play an even greater role over time.

8.5. Moreover, a digital asset can be coded in such a way that its negotiability is limited in fact. For example, a digital asset could either directly or indirectly display information that puts prospective purchasers on notice of the possible existence of conflicting claims. This would be the case, for example, if a digital asset were programmed so that its metadata clearly specified the identity of its legitimate owner and expressly stated that anyone considering acquiring it should deal with that person.

8.6. In relation to the operation of the innocent acquirer rule in Principle 8 to linked assets, see Commentary 4.11 and 4.29 to 4.32.

Principles 8(1) to 8(3)

8.7. Principle 8(1) sets out the requirements for a transferee to be an innocent acquirer. The first is that the transferee must obtain control, as defined in Principle 6. The second is that the innocent acquirer must comply with the requirements specified by the relevant State (that is, the State whose domestic law is the applicable law). As indicated by Principle 8(1)(b), a State has flexibility as to the precise contours of the requirements for innocent acquisition of digital assets that it adopts, given that such requirements need to be consistent with the good faith acquisition and take free rules of that State for other types of assets. A State might wish to adopt slightly different innocent acquisition rules for different types of digital assets (see also Commentary 3.7).

8.8. As discussed in Commentary 8.1 and 8.2 above, Principles 8(2) and 8(3) set out the consequences of a transferee being an innocent acquirer.

Principle 8(4)

8.9. Principle 8(4) is intended to make clear that, for example, even if an acquirer receives control of a digital asset by a change of control made by a thief or a 'hacker', the acquirer may qualify as an innocent acquirer. See also the discussion in Commentary 6.6, 6.9 and 6.10.

Principle 8(5)

8.10. Principle 8(5) provides a default set of requirements for a transferee to be an innocent acquirer for use if, first, a State's court needs, in the course of litigation, to apply the Principles pursuant to one of the choice-of-law rules in Principle 5(1)(a), 5(1)(b) or 5(1)(d) and, second, that State has not yet adopted its own innocent acquisition rule for digital assets of the relevant type. If the State has adopted its own rule, that rule would apply as Principles law. Principle 8(5) is drawn substantially from the innocent acquisition rule in the Geneva Securities Convention.

Principle 8(6)

8.11. Principle 8(6) reflects Principle 3(3), which states that, except as displaced by these Principles, other law continues to govern issues relating to a digital asset. However, this is subject to Principle 9.

Principle 9

Rights of a transferee

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

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

Commentary

Principles 9(1): nemo dat rule

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

Principle 9(2): shelter rule

9.2. Principle 9(2) states the shelter principle: a transferee acquires all the proprietary rights of the transferor that were transferred or that the transferor had the power to transfer. However, Principle 9(2) makes it clear that if a transferor transfers less than all of its proprietary rights in the digital asset, the transferee acquires only the proprietary rights that were transferred.

9.3. Pursuant to Principle 9(2), a transferee from a person that was an innocent acquirer of proprietary rights in a digital asset and any subsequent transferee acquires the rights of the innocent acquirer, that

is, rights free from conflicting proprietary rights and the successful assertion of conflicting proprietary claims. This is the case even though the transferee at the time of the transfer would not itself meet the applicable requirements as an innocent acquirer (*e.g.*, if it had the knowledge specified in Principle 8(5)(a), if applicable, with respect to the digital asset).

SECTION IV: CUSTODY

Principle 10

Custody

(1) In these Principles:

(a) 'custodian' means a person who provides services to a client pursuant to a custody agreement as defined in paragraphs (3) and (4), and is acting in that capacity;

(b) 'sub-custodian' means a custodian who provides services to another custodian pursuant to a custody agreement as defined in paragraphs (3) and (4), and is acting in that capacity;

(c) 'client' means a person to whom a custodian provides services pursuant to a custody agreement as defined in paragraphs (3) and (4).

(2) A custodian 'maintains' a digital asset for a client if:

(a) that custodian has control of the digital asset; or

(b) that custodian enters into a custody agreement, as defined in paragraph (3), with a sub-custodian with respect to the digital asset in the circumstances set out in Principle 11(4).

(3) Subject to paragraph (4), an agreement for services to a client in relation to a digital asset is a 'custody agreement' if:

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

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

(c) the client does not have the exclusive ability to change the control of the digital asset within the meaning of Principle 6(2).

(4) An agreement to which paragraph (3) applies is not a custody agreement if it is clear from the agreement that, if the service provider enters into an insolvency-related proceeding, the digital asset would be part of the service provider's assets available for distribution to its creditors.

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

Commentary

General

10.1. The purpose of Section IV is to set out private law principles relevant to custody of digital assets. Other law, including regulatory law, may also apply to the provision of custody services. Custody, broadly speaking, is where a person (usually a legal person, which may be a regulated entity), maintains a digital asset on behalf of and for the benefit of another, a client (which may be another custodian), in a manner that gives the client special protection against unauthorised dispositions of the asset and against the insolvency of the custodian who maintains the digital asset. It only applies where the person providing the custody services does so in the ordinary course of its business. The special protection for the client referred to is likely to be achieved in private law by the client having a proprietary right of some sort in the asset, although the precise technique by which this protection is achieved will vary according to the private law of the relevant jurisdiction. As mentioned in Commentary 6.5 and 6.6, custody is an example of a situation where one person may have

control (as defined in Principle 6) of a digital asset while another person (the client) may have a proprietary right in that asset.

10.2. It is quite common that the same service provider carries out various activities other than custody, including trading digital assets for its clients, trading digital assets on its own account, operating a marketplace ('exchange' or 'trading platform'), etc. Principle 10 only applies to the service of custody, irrespective of other activities carried out by the person providing this service and irrespective of the provider's regulatory status. Wherever the word 'custodian' is used, it refers to that person insofar as it is acting the capacity of custodian. Whatever Principle 10 states about custodians only applies to custody services and not to other services provided by those persons.

10.3. Whether the services provided by a provider are custody services will depend on whether the agreement between the service provider and its client is a custody agreement. Principle 10(3) defines a custody agreement. Principle 10(1) defines the important parties in relation to custody. The person controlling the asset is either a 'custodian' (in which case it controls the assets for a 'client' who is not a custodian) or a 'sub-custodian' (in which case it controls the asset for a client who is a custodian, and who has entered into a custody agreement with a client in relation to that asset). A sub-custodian is also a custodian within the definition in Principle 10(1).

Maintaining a digital asset

10.4. The purpose of Principle 10(2) is to introduce the concept of 'maintaining' a digital asset, which is wider than the (factual) concept of 'control' as defined in Principle 6. The word 'maintain' is defined as encompassing two situations in which a custodian 'maintains' a digital asset for a client. The first is where a custodian has control of an asset within the meaning of Principle 6. The second is where a custodian is the recipient of custody services, that is, where another custodian (a sub-custodian) is obliged to control the asset for that custodian. Where a sub-custodian is used, the sub-custodian and the custodian both 'maintain' the asset. In this situation, the custodian enters into a custody agreement with the sub-custodian and becomes its client. The custodian, therefore, has rights against the sub-custodian under that custody agreement. There could also be more

than one layer of custodians. For example, if there were three layers, the sub-custodian itself 'maintains' the asset for the custodian, because a third custodian is obliged to control the asset for that sub-custodian.

Custody agreement

10.5. Principles 10(3) and 10(4) provide a method to identify whether an agreement is a custody agreement or not. They perform two functions.

10.6. First, sub-paragraphs (a), (b) and (c) of Principle 10(3) serve as a definition of a custody agreement, and therefore of custody. Sub-paragraph (a) makes it clear that to be a custodian, a service provider must be acting in the ordinary course of its business. Sub-paragraph (b) sets out the core duty of a custodian (see also Principle 11(1)). It covers three situations. The first is where the custodian, having entered into a custody agreement with the client, does not control the digital asset which is the subject matter of the agreement, for example, (a) if the client has not yet transferred a digital asset to the custodian or the custodian has not yet received it for the client, (b) if the custodian has exercised a right of use (see Principle 11(1)), or (c) if the custodian in is breach of its obligations and fails to control the digital asset that is the subject of the custody agreement. In each of these examples, the custodian is obliged to obtain the digital asset which is the subject of the agreement. If the digital asset is treated as fungible (see Commentary 11.6), the obligation will be to obtain a digital asset of the description specified in the agreement. The second situation is where the custodian does control the digital asset, in which case the custodian is obliged to continue to control that digital asset until otherwise instructed by the client or until the custodian exercises its right of use, if it has one (see Principles 11(1)(a) and 11(1)(b)). The third situation is where a custodian does not control the digital asset itself, but is the recipient of custody services, that is, where a sub-custodian controls the asset for that custodian. In the second and third situations the custodian 'maintains' the digital asset as defined in Principle 10(2). Principle 10(3)(c) makes it clear that an agreement is not a custody agreement if the client has the exclusive ability to change the control of the digital asset (for the meaning of 'change of control', see Principle 6(2)). This situation is discussed in Commentary 10.14

to 10.19. The exclusive ability referred to in Principle 10(3)(c) is that referred to in Principle 6(1)(a)(iii) and therefore is subject to the relaxation of the concept of 'exclusivity' set out in Principle 6(3).

10.7. The second function of Principles 10(3) and 10(4) is to address the line between a custody agreement and an agreement under which any assets maintained by the service provider form part of that service provider's assets available for distribution to its creditors if it enters into an insolvency-related proceeding (such an agreement is discussed in Commentary 10.20). This latter type of agreement can look similar to a custody agreement, as both are situations in which the client does not have control of the digital asset, and the service provider maintains an account in which the client's entitlement is recorded (a record of client entitlement is also (or should be) kept under a custody agreement, see Principle 11(3)(a)). However, under this type of (non-custody) agreement the client is exposed to the insolvency risk of the account provider. A client taking on such a risk should be aware that it is doing so, whereas the risk is not present under a custody agreement (as long as the custodian fulfils its obligation to maintain the digital asset). For this reason, an agreement under which the client does not have control is presumed to be a custody agreement unless it is made clear in the agreement that assets held by the service provider form part of the service provider's assets available for distribution to its creditors if it enters into an insolvency-related proceeding (see Principle 13(2)). It is not necessary for this, or any particular, form of words to be used as long as this consequence is clear to clients. Principle 10(4) is designed to act as an incentive to service providers to make the nature of the agreement clear on its face.

10.8. A state may wish to protect a client who enters into a non-custody agreement which exposes the client to the insolvency risk of the service provider. Various examples of such regulatory protection are set out in Commentary 10.21.

Principle 10(5)

10.9. Principle 10(5) makes it clear that, without affecting the existence or operation of the custody relationship, the client could be acting on behalf of a third party in any capacity. This could cover situations such as agency or nomineeship, and could also include

where the client (in the relevant jurisdiction) holds the asset on trust for someone else (*e.g.*, the client could be an investment fund or an individual holding the asset for a family member) or that the functional equivalent could occur in other jurisdictions.

Illustrations of custody

10.10. There now follow two illustrations of situations in which the relationship between the service provider and the client is one of custody, which are to be read in comparison with the examples of non-custody in Commentary 10.13 onwards. The first illustration of custody is a general description of a custodial wallet (sometimes called a hosted wallet) and the second is a specific illustration of where such a service could be provided within a wider context. The term 'wallet' in the following illustrations is used in the colloquial sense in which it is used in the market, that is, software (or hardware) that enables a person to interact with a digital asset, for example, via the generation and management of public and/or private keys. The means by which, and by whom, this interaction is effected depends on the type of wallet. As provided in Principles 10(3) and 10(4) and Commentary 10.7, an agreement between a client and a service provider in the context set out in Commentary 10.11 and 10.12 will be a custody agreement unless it is made clear that the assets controlled by the service provider form part of the service provider's assets available for distribution to its creditors if it enters into an insolvency-related proceeding, in which case the agreement falls within the illustration discussed in Commentary 10.20.

Custodial or hosted wallet

10.11. ***Illustration 1.*** In a custodial or hosted wallet arrangement, users transfer digital assets to the wallets of a service provider. The service provider (the custodian) holds the private keys of the wallet to which the digital asset is thereafter connected. Hosted wallets often appear in the context of trading platforms, where an intermediary facilitates trades of digital assets between users. An example of the provision of hosted wallet services as part of a trading platform service is given in Commentary 10.12. Service providers often offer more than one kind of wallet service, allowing users to take advantage of both self-custody and custodial wallet solutions (for self-custody see

Commentary 10.15 to 10.17) because the two different types of wallets serve different purposes.

Trading account

10.12. ***Illustration 2.*** A, a service provider, offers what it terms a 'trading account', which is the functionality within a wallet that enables a user to buy and hold all digital assets purchased with fiat currency through A. The contract between A and its client expressly provides that title to the digital assets in the trading account belong to the user and does not transfer to A, and emphasises that digital assets in the trading account are not the property of A and are not loaned to A. Some transactions between A's clients initiated from a trading account occur off-chain, and are recorded only by accounting ledger entries in the records of A. A transaction between a self-custody wallet (provided by A or by another service provider) and a trading account provided by A, on the other hand, would occur on-chain.

Illustrations of non-custody arrangements

10.13. There are a number of situations where a person controls a digital asset which are not custody and where any agreement with a service provider is not a custody agreement, as defined in Principles 10(3) and 10(4). The following paragraphs describe and illustrate examples of these situations.

10.14. ***Illustration 3: Where a person, such as an investor, controls a digital asset.*** A person (such as an investor) can control a digital asset by using some hardware or software. This is the case where, for example, she runs a full node (or a light node) on the blockchain on which the asset is registered or where she uses wallet software or service to access the blockchain. In all these cases, the investor keeps control of the digital asset because she stores and uses the private key and does not entrust or surrender it to a third party. The provider of the wallet used by the investor only provides the means (hardware or software) by which the investor stores and uses her private keys. The investor is exposed to the risk of the wallet malfunctioning, but her digital assets are not controlled by the provider. The insolvency of the provider would affect its ability to operate or maintain the wallet but has no legal impact on the digital

assets controlled by the investor. The relationship between the investor and the person providing the hardware or software is purely contractual and is governed by the terms of the agreement between them.

10.15. Self-custody is where a user holds private keys either using software solutions deployed directly on their own computer or mobile phone, or using cloud-based software-as-a-service non-custodial wallets. The two options are quite similar: the chief difference is in the location where the private keys are held. In both cases, the client controls the digital asset. The two options are illustrated in the following two paragraphs.

Self-custody by wallet software

10.16. ***Illustration 4.*** 'Self-custody' in this paragraph refers to the use of wallet software, of which an example is given in this paragraph. 'XX' is open source software, developed by a global community of developers and designers. It is compatible with a variety of hardware wallets. The user of XX creates a wallet password and secret recovery phrase, which are stored, together with the private keys, in an encrypted format on the mobile phone or computer on which the XX software is installed. Transactions conducted through wallets using XX software are broadcast on-chain.

Self custody by cloud-based software-as-a-service

10.17. ***Illustration 5.*** Y, a service provider, provides a non-custodial wallet for users. A user creates an account, and creates a password, which gives the user access to an encrypted file kept by Y on the blockchain containing a 'seed' (a secret private key recovery phrase), the users' private keys and addresses of digital assets. The password is not stored by Y and must be kept safe and confidential by the user herself. Y has no access to the user's private keys, seed, or password. When a password or seed phrase is used correctly, the file containing private keys is decrypted locally on the user's computer or mobile phone, and the user can carry out transactions, which are conducted directly on-chain. Y stores the encrypted file in the cloud, while when the XX software is used (see Commentary 10.16), the encrypted file is stored locally on the user's computer or mobile phone. Users of the

software-as-a-service model, therefore, could find themselves in difficulty should Y ever decide to stop providing the wallet services.

Safeguarding of private keys

10.18. ***Illustration 6: Where a business provides safeguarding of private keys.*** Another arrangement is where a provider safeguards its client's private keys or provides software or hardware to facilitate the client's safeguarding its private keys. Depending on the features, the provider of the software or hardware may (or may not) have the ability to use the client's private keys and thus take control of the client's digital assets. However, this is not the purpose of this type of arrangement and typically the provider 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)(iii)). This business model is therefore not a custody service as defined in Principle 10, even though it is sometimes called 'custody' by market participants. In contrast, where a service provider provides a custody service, its clients transfer their digital assets to addresses or private keys controlled by that service provider, or the service provider acquires digital assets which it controls for the client. An example of safeguarding of private keys follows in the next paragraph.

10.19. The Z wallet generates private keys within the device, and then stores the keys there. This provides very secure cold wallet storage, by keeping the keys unconnected, and thus out of reach from online hackers and other threats, from the moment of generation until the moment of use. The software on the Z hardware is not intermediated, as no third-party intermediary has access to the keys held on the Z wallet. When a user wants to transact with the keys held in a Z wallet, they use software similar to a mobile phone app store to access services provided by other providers to send, buy, or sell digital assets.

Agreement for delivery of digital assets

10.20. ***Illustration 7: An agreement for delivery of digital assets.*** 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 in the primary or secondary market for the client. The firm or institution will maintain an account (similar to a bank account, as opposed to the bailment or custody of assets belonging to the client) 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 insolvent, the claim for the 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, although in some jurisdictions distribution of digital assets themselves may be permitted. If the digital asset is not fungible, the relevant claim is for delivery of a specific asset rather than for a generic quantity of digital assets of a certain description. This, however, should not alter the legal characterisation of the obligation as a personal right or its treatment as an unsecured claim in the insolvency of the obligee.

10.21. A State may consider whether regulatory law should mitigate the risk for some or all types of clients who enter into the type of agreements described in Commentary 10.20. One example would be a requirement for providers of this type of account to hold a certain amount of capital. Another example would be a requirement to hold liquid assets commensurate to the value of digital assets that the provider owes to its clients, which may be accompanied by a preference over such assets for the clients on the insolvency of the account provider. Other examples are a requirement for specific disclosure of the relevant risks in the agreement, a requirement that providers of this type of account must be regulated entities conforming to standards, or a limitation on the type of people who can become clients (as in many crowd-funding regulations).

Decentralised autonomous organisations

10.22. Decentralised autonomous organisations (DAOs) use code (also called smart contracts or apps) stored and executed on a 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 self-custody, custody, and a personal claim as described in Commentary 10.20 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 a trust, 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. For the reasons given in this paragraph, a structure involving a DAO is unlikely to involve custody, but this will depend on the specific arrangement in each case.

Principle 11

Duties owed by a custodian to its client

(1) A custodian owes the following duties to its client in relation to a digital asset it maintains for that client:

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

(b) the custodian is obliged to comply with an instruction given by the client to transfer the digital asset, unless:

(i) the custodian is prohibited from complying with the instruction by other law or by any agreement between the custodian and a third party to which the client is a party or has consented;

(ii) the custodian is not obliged, by other law or by an agreement with the client, under certain circumstances, to comply with the instruction;

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

(2) Unless prohibited by the custody agreement or by other law, a custodian may maintain digital assets of the same description for two or more of its clients as an undivided pool.

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

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

(b) the duty at all times to securely and effectively maintain digital assets in

accordance with the records it keeps for its clients;

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

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

(e) subject to any right granted to the custodian or to another person, the duty to pass the benefits arising from digital assets to the client for whom it maintains those assets.

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

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

(a) granted to that custodian by the client;

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

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

Commentary

Principle 11(1)

11.1. Principle 11(1) sets out duties which are owed by a person providing custody services under an agreement with a client. These are basic duties and a State should not permit them to be excluded by the terms of the custody agreement. If the custodian is a sub-custodian, the sub-custodian's client is itself a custodian.

11.2. The duty in Principle 11(1)(a) refers to the inability of the custodian to use the digital asset for its own benefit except as

permitted by the client and by other law (as defined in Principle 2(4)). The client may consent to that use either by contract or by an instruction to the custodian, and may consent to a use more limited than that permitted by other law. The other law of a State may permit a custodian to have a right of use in respect of digital assets in relation to which it provides custody services: this permission may be contained in regulation and/or in private law. In the latter case, the extent of the permission may depend on the way in which a custody relationship is characterised by that private law.

11.3. The duty in Principle 11(1)(b) makes the basic point that a custodian is a person who must deal with the digital asset according to the client's instructions. However, this obligation is qualified by any prohibition on such dealing to be found in other law, including criminal or regulatory law, or any agreement made between the custodian and any third party to which the client is a party or has consented. If the client has granted the custodian a security right in the digital asset, or any such security right has arisen by operation of law, this will also qualify the custodian's obligation (see Principle 11(5)). Moreover, other law, or the agreement with the client, may specify particular circumstances in which the custodian is not obliged to comply with the client's instructions. This would further qualify the basic obligation.

11.4. Principle 11(1)(c) makes it clear that the custodian must owe to the client some duties in relation to safeguarding of the digital asset. Safeguarding includes the attainment of the result set out in Principle 13(2) (that the assets safeguarded are not to be part of the assets available for distribution to the custodian's creditors if it enters into an insolvency-related proceeding). The details of these safeguarding duties will typically be included in the custody agreement. A State can choose which private law safeguarding duties should be imposed on a custodian, and therefore cannot be excluded by agreement. Some suggestions for States are contained in Principle 11(3).

11.5. The language of Principle 11(1) is intended to be functional and neutral between legal cultures. In some jurisdictions, the relationship between custodian and client will be legally characterised as a trust while in other jurisdictions it may be characterised as a contractual or other type of legal relationship.

Principle 11(2)

11.6. Principle 11(2) addresses the common situation where a custodian maintains digital assets of the same description for several clients. The phrase 'of the same description' is used in these Principles to refer to digital assets that are treated by market participants as fungible (see also Principles 13(5) to 13(7)). Fungibility is not a technical characteristic of a digital asset, but a matter of market practice. The record of any unit (or quantity) of a digital asset in a digital ledger is individualised because it is, by definition, capable of control, see Principle 2(2). However, as a matter of market practice, many digital assets (such as cryptocurrencies) are treated as fungible so that any such unit or units will satisfy an obligation to deliver the digital asset.

11.7. Subject to other law or to the custody agreement, Principle 11(2) permits a custodian to maintain digital assets for several clients as an undivided pool. This has two consequences. First, the custodian may control an undivided pool of client assets using one or more private keys, so that no specific unit or quantity of that digital asset is specifically allocated to a particular client. If the custodian maintains digital assets for several clients with a sub-custodian, maintaining them as an undivided pool means that the custodian need not have a separate sub-account with the sub-custodian for each client. As a result, for any particular digital asset, an undivided pool includes all digital assets of that description controlled by the custodian for its clients using one or more private keys as well as all digital assets of that description maintained with one or more sub-custodians. Second, when the custodian receives an instruction of a client in respect of a digital asset maintained for its clients as an undivided pool, it may comply with that instruction using any unit or quantity of such digital asset that it controls directly or that it maintains with a sub-custodian. This is because these various units or quantities of the digital asset are all of the same description, *i.e.*, they are treated as fungible, as explained above in Commentary 11.6. Where the custodian is not allowed to maintain an undivided pool, it must implement what is often called full segregation. The reference to 'a custodian' in Principle 11(2) also applies to a sub-custodian, whose clients are custodians.

Principle 11(3)

11.8. Principle 11(3) sets out private law duties which a State may wish to ensure are owed by a custodian to its client, although it is for a State to choose whether it wishes to do so, in which case it would have to make the chosen duties mandatory and non-excludable by agreement. Separately, a State may wish to impose these duties on custodians as a matter of regulatory law, that is, by imposing duties for which there is no private law redress but breach of which may incur sanctions imposed by the State. Again, it should be recalled that if the custodian is a sub-custodian, the client is a custodian. For the result of Principle 13(2) to be attained under some domestic laws, the duty under Principle 11(3)(d) must not be permitted to be excluded by the terms of the custody agreement. A State may choose to impose a similar duty as a matter of regulatory law.

11.9. The duty in Principle 11(3)(a) is that a custodian must keep a record of the digital assets it maintains for every client. That record may either be kept separately from the distributed ledgers which record the respective digital assets or, if technology allows, be part of the information stored in the distributed ledger.

11.10. The duty in Principle 11(3)(b) is that the custodian owes a duty to maintain assets correlating to those records. Thus, if the record shows that a custodian maintains 1 bitcoin for A, the custodian must maintain at least 1 bitcoin.

11.11. The duty in Principle 11(3)(c) is to replace any missing assets, in other words, to reconcile what the custodian actually maintains to the client records. The assets acquired must, of course, be of the same description and in the same quantity as the assets recorded in the records.

11.12. The duty in Principle 11(3)(d) relates to the custodial duty to separate client assets from house assets (*i.e.*, the custodian's own assets). A custodian may separate its clients' digital assets from its own by controlling them using different private keys or by maintaining them on different accounts with a sub-custodian. The legal effect of this depends on the applicable law.

11.13. Principle 11(3)(d) does not address the segregation of assets of any particular client. Rather than maintaining client assets of the same description as an undivided pool, a custodian may offer to a client the possibility of the custodian maintaining the assets of that client separately from the assets of the same description of other clients (so-called full segregation). That would require the custodian to control the client's assets using a separate private key or to maintain them in a separate account with a sub-custodian so that such assets are exclusively allocated to the client. The legal effect of such arrangement will depend on the applicable other law, and may vary from jurisdiction to jurisdiction.

11.14. The duty in Principle 11(3)(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, monetary dividends, distributions in kind (*e.g.*, 'airdrops'), and additional digital assets that may be created as a result of a network-wide event such as a 'fork'.

Principle 11(4)

11.15. Principle 11(4) makes it clear that a sub-custody structure, can be used. Under this structure, the custodian maintains the digital asset by entering into a custody agreement with a sub-custodian with respect to that asset (see Principle 10(2) and Commentary 10.4). Such a structure can be used if the sub-custodian is bound by the duties set out in Principle 11. A custodian would, however, be in breach of its own duties to the client if the sub-custodian was not subject, in the sub-custody agreement, to the mandatory and non-excludable private law duties of a custodian under the applicable law. These duties are those set out in Principle 11(1) plus those listed in Principle 11(3) that the relevant State has chosen to make mandatory. Other law determines the extent to which, if any, a custodian is responsible to its client with regard to the non-performance by the sub-custodian of its duties under Principle 11 and the sub-custody agreement.

Principle 11(5)

11.16. Principle 11(5) recognises that a custodian may have a security right in the digital asset it maintains for a client. For example, the client

may owe the custodian fees, for which the custodian wishes to be secured, or the custodian may have lent the client money to acquire the digital asset. A security right under Principle 11(5)(a) would be made effective against third parties by control under Principle 15, since the custodian either controls the digital asset itself or has entered into a custody agreement with a sub-custodian in relation to the asset. A client can also grant a security right in a digital asset maintained by a custodian to a third party (this follows from the nature of a digital asset set out in Principle 3(1) and Principle 14(1)). However, in that case either the secured creditor would need to make the security right effective against third parties by control under Principle 15 by the custodian maintaining the digital asset for the secured creditor or it would need to make the security right effective against third parties by a means (available under other law) other than control.

Principle 12

Innocent client

(1) Subject to paragraph (2), where a custodian maintains a digital asset pursuant to a custody agreement as defined in Principles 10(3) and 10(4), no rights based on a proprietary claim to that asset may be successfully asserted against the client.

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

(3) If digital assets are maintained by a custodian for two or more clients as an undivided pool, paragraphs (1) and (2) apply to each client for whom the digital assets are maintained.

Commentary

12.1. Principle 12 addresses the situation where a custodian or sub-custodian obtains control of a digital asset and maintains that asset for a client, or, if the asset is maintained as an undivided pool, for a group of clients (the latter situation is addressed in Commentary 11.6 and 11.7 and in Principle 11(2)). Principle 12 provides that the client cannot be subject to a successful claim to that asset brought by a person whose rights are violated by the change of control to the custodian, unless the client knows or ought to have known of that violation of rights. It is, therefore, an adaptation of the innocent acquisition rule tailored for the circumstances of custody. The standard of 'innocence' is that set out in Principle 8(5)(a), although, in accordance with Principle 8(1)(b), a State has flexibility to adapt this standard to be consistent with its own good faith purchase and take free rules. Principle 12 does not address the situation where the client itself has granted a right in the digital asset to a third party.

12.2. Principle 12 applies at each level of custody, if there is more than one level. Thus, if a sub-custodian maintains a digital asset for a custodian (who then maintains that digital asset for a client, see Principle 10(2)), Principle 12(1) applies to that custodian as client (vis-à-vis the sub-custodian). Principle 12(1) also then applies to the client of the custodian because the custodian maintains that digital asset for that client.

12.3. There are a number of ways in which a custodian could come to obtain control of a digital asset for a client. Depending on the factual situation and the manner in which the applicable law analyses that situation, the position of the client is governed either by Principle 8 or Principle 12. Some illustrations of possible situations are set out in the next paragraphs.

12.4. ***Illustration 1.*** A custodian obtains control of a digital asset in the course of a transfer of that asset to it for its own account and the custodian is an innocent acquirer under Principle 8, since the relevant requirements are satisfied. Later, as part of a subsequent sale transaction, the custodian transfers the digital asset to a client, and maintains it for that client. In this situation, there would be no need for Principle 12 to apply. This is because, under Principle 9(2) no successful claims in respect of the asset could be made against the custodian, and therefore no successful claims could be made against the client for whom the custodian maintained that digital asset. Principle 9(2) provides that a transferee acquires all the proprietary rights that its transferor had.

12.5. ***Illustration 2.*** If a client instructed its custodian to obtain a digital asset on its behalf, in circumstances where the custodian acted purely as an agent or representative of the client, it is likely that the client would also qualify as an innocent acquirer under Principle 8 if the control by the custodian was treated as that of the client and the client otherwise satisfied the requirement for innocent acquirer status.

12.6. ***Illustration 3.*** If a custodian obtained control of a digital asset in circumstances other than those in Illustration 2 in order to maintain it for a client (or a number of clients in the case of digital assets to be held as an undivided pool (see Principle 11(2)) Principle 12 would apply.

12.7. Principle 12 applies equally whether or not the digital asset is part of an undivided pool maintained for several clients. As stated in Principle 12(3), where digital assets are maintained as an undivided pool, Principle 12 applies to each client in the same way. Thus, unless a client knows or ought to know of another person's violated right to a digital asset which forms part of the pool, no claims can be asserted against that client in respect of that digital asset or any others in the pool. Principle 12 does not affect the position of the clients in the pool with respect to each other, which is that all clients share rateably and proportionately in the pool, including in the case of insolvency of the custodian (see Principles 13(5) and 13(7)).

Principle 13

Insolvency of a custodian and creditor claims

(1) A digital asset that a custodian maintains for a client under a custody agreement is not available for the satisfaction of claims of creditors of the custodian.

(2) If a custodian enters into an insolvency-related proceeding, a digital asset that it maintains for a client under a custody agreement does not form part of that custodian's assets available for distribution to its creditors.

(3) If a custodian maintains a digital asset for a client with a sub-custodian, and the custodian enters into an insolvency-related proceeding, the rights it has against the sub-custodian in respect of that digital asset do not form part of the custodian's assets available for distribution to its creditors.

(4) If a custodian enters into an insolvency-related proceeding, the insolvency representative must take reasonable steps:

> **(a) for the control of a digital asset maintained for the custodian's client to be changed to the control of that client or of a custodian nominated by that client;**
>
> **(b) for any rights the custodian has against any sub-custodian in respect of a digital asset maintained for the custodian's client to be transferred or otherwise made accessible to that client, including through transfer to another custodian nominated by that client.**

(5) Paragraphs (6) and (7) apply if all of the following requirements are fulfilled:

> **(a) a custodian enters into an insolvency-related proceeding;**

(b) digital assets of the same description are maintained by the custodian for two or more clients as an undivided pool; and

(c) the quantity of digital assets maintained by the insolvent custodian for those clients is less than the aggregate quantity of digital assets of the same description that it is obliged to maintain for those clients ('shortfall').

[(6) The shortfall is met first by any digital assets of the same description maintained by the custodian for itself.][2]

(7) Any [remaining] shortfall shall be borne by the clients for whom the custodian maintains the digital assets as an undivided pool, in proportion to the respective quantity of digital assets of the same description that the custodian is obliged to maintain for those clients.

(8) If a custodian maintains a digital asset for a client with a sub-custodian, and the sub-custodian enters into an insolvency-related proceeding, the custodian must seek to obtain control of that digital asset from the insolvency representative or to maintain the digital asset with another sub-custodian.

Commentary

Principle 13(1)

13.1. Principle 13(1) applies where the custodian has not entered into an insolvency-related proceeding. It makes it clear that digital assets maintained by a custodian for a client are not available for the satisfaction of the claims of the custodian's creditors. This result

---

2 Principle 13(6) is an optional provision which a State may choose to adopt. If it does so, the word 'remaining' in Principle 13(7) would need to be retained.

parallels the substance of paragraph (2), which provides that digital assets maintained for clients are not part of the assets available for distribution to the custodian's creditors if it enters into an insolvency-related proceeding. These provisions reflect the baseline concept that such digital assets belong to the clients, not to the custodian.

Insolvency-related proceeding

13.2. Principles 13(2) to 13(8) apply if a custodian enters into an insolvency-related proceeding. 'Insolvency-related proceeding' is defined in Principle 2(6), but it should be borne in mind that a State might specify a special type of insolvency regime for certain types of financial institutions, which could include some custodians of digital assets. If this is the case, and the special regime does not fall within the definition in Principle 2(6), a State will need to modify the definition of insolvency-related proceeding in relation to those custodians accordingly. Similarly, if the consequences set out in Principle 13 would not be possible under the special regime, Principle 13 will need to be modified accordingly.

Principle 13(2)

13.3. Principle 13(2) 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, digital assets it maintains for clients as custodian are not part of the assets available for distribution to its creditors. If, on the other hand, a service provider is not a custodian because its agreement with the client is an agreement for the delivery of digital assets (see Illustration 7 in Commentary 10.20), any assets it controls will usually be part of its assets for distribution to its creditors. A service provider could be a custodian in relation to some clients ('act in that capacity' within the meaning of Principle 10(1)), and not a custodian in relation to other clients (because the agreement is of the type mentioned in the previous sentence). The effect of Principles 10(3) and 10(4) is that any agreement which has the three characteristics of a custody agreement set out in Principle 10(3) will attract the consequences in Principle 13(2) unless the agreement makes it clear that this is not the case. In Principle 13(2), the 'custodian' could in fact be a sub-custodian and the 'client' could be a custodian.

Principle 13(3)

13.4. Principle 13(3) sets out the consequences when a digital asset is held through a sub-custodian (see Principle 11(4)). As explained in Commentary 10.4, when a custodian maintains a digital asset through a sub-custodian, the custodian (who will be the client of the sub-custodian under a custody agreement) has rights against that sub-custodian under the custody agreement. If the custodian is insolvent, its rights against the sub-custodian are not part of the custodian's assets available for distribution to its creditors.

Principles 13(4) to 13(7)

13.5. Principles 13(4) to 13(7) give guidance as to suitable rules which should (or, in the case of Principle 13(6), could) apply in relation to digital assets (or if a sub-custodian is used, rights against the sub-custodian) if a custodian enters into an insolvency-related proceeding. These rules are not comprehensive; the applicable insolvency law governs all other issues that could arise in these circumstances. It should be noted that a custodian or sub-custodian could have a security right over, or another type of right to, digital assets maintained for its clients (see Principle 11(5)). The effect of this on the actions taken by an insolvency representative would be a matter of other law.

13.6. Principle 13(4) imposes a duty on the insolvency representative to take reasonable steps so that the client can obtain the digital assets maintained for it by the custodian. If the digital assets are maintained by the custodian by entering into a custody agreement with a sub-custodian (Principle 10(2)(b)), the duty on the insolvency representative relates to the custodian's rights against the sub-custodian. The client may want to obtain control of the digital assets (or obtain the rights against the sub-custodian) itself, or may want another custodian to maintain them on its behalf. The insolvency representative may need to take certain steps to achieve this result, such as obtaining the private key(s) relating to those digital assets.

13.7. Principles 13(5) to 13(7) apply where digital assets of the same description are maintained by a custodian for its clients as an undivided pool (see Principle 11(2) and Commentary 11.6). Undivided

pools of digital assets of the same description are explained in Commentary 11.6 and 11.7. A custodian can maintain digital assets as an undivided pool either by controlling the assets itself or by entering into a custody agreement with a sub-custodian in respect of an undivided amount of digital assets. In this latter situation, its rights against the sub-custodian will be undivided. Principles 13(5) to 13(7) deal with the situation where there is a shortfall of digital assets, or rights against the sub-custodian, of a particular description. Principle 13(5) explains the situation of shortfall. In the insolvency-related proceeding of a custodian, there may be potentially as many shortfalls as there are undivided pools.

13.8. If there is a shortfall, a State may wish to provide that the loss is first met by any digital assets of the same description maintained by the custodian on its own account, whether by controlling those assets itself or by use of a sub-custodian. This approach follows that of Article 25 of the Geneva Securities Convention. However, under that Convention, a State can make a declaration that this rule is not to apply in that State. In a similar way, it is a policy decision for a State whether or not to adopt the rule set out in Principle 13(6). For this reason, Principle 13(6) is in square brackets.

13.9. Under Principle 13(7) the loss of digital assets (or rights against a sub-custodian) caused by the shortfall should be borne *pari passu* by all the clients for whom the custodian is obliged to maintain the assets of which there is a shortfall. In other words, if there is a shortfall of digital asset A and/or rights against any sub-custodian that relate to digital asset A, and none in respect of digital asset B, the shortfall in respect of A is shared rateably among all clients for whom the custodian is maintaining an undivided pool of A. The approach follows that of Article 26(2) of the Geneva Securities Convention. If a State chooses to adopt the rule in Principle 13(6), then the word 'remaining', which is in square brackets in Principle 13(7), applies. Otherwise, that word is not required.

Principle 13(8)

13.10. Principle 13(8) sets out the consequences of the insolvency of a sub-custodian when a digital asset is maintained through that sub-custodian (see Principle 11(4)). In these circumstances, the custodian

must seek to change control of the digital asset from the insolvent sub-custodian, either to itself or to another sub-custodian. If the custodian is insolvent, its rights against the sub-custodian under the custody agreement do not form part of its assets available for distribution to its creditors.

SECTION V: SECURED TRANSACTIONS

Principle 14

Secured transactions: general

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

(2) If a digital asset is linked to another asset, other law applies to determine the legal effect on that other asset of the creation of a security right in that digital asset.

(3) If a digital asset is linked to another asset, other law applies to determine the legal effect on that other asset of a security right in that digital asset being made effective against third parties.

Commentary

Principle 14(1)

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

14.2. Section V applies to transactions under which a security right in a digital asset is granted to a secured creditor to secure the performance of any existing, future, or contingent obligations of the grantor or another person. These transactions, covered by Section V, are called 'secured transactions' in the Commentary to Section V. The Principles in Section V are not intended to interfere with domestic law conceptions of security right or domestic security law, except to the extent that such law should be changed to deal specifically with

security over digital assets. Many proprietary aspects concerning security rights are governed by other law (see Principles 3(3)(c), 3(3)(e) and 3(3)(g)). The Principles presuppose the existence of some rules (such as the existence of methods other than control of making a security right effective against third parties (which is presupposed by Principle 16) or the requirement to notify the grantor and third parties prior to disposal of a digital asset in enforcement of a security right) and explain how those rules would operate in the context of enforcing security rights in digital assets.

14.3. The Principles are not only for those States that have implemented the UNCITRAL Model Law on Secured Transactions or a law based on approaches similar to the UNCITRAL model. Therefore, the type of transactions which fall within the category of 'secured transactions' and the types of rights which fall within the term 'security right' will depend on the applicable domestic law. For example, the term 'secured transactions' will typically include transactions creating various types of 'security rights', such as pledges, charges, or security assignments. It may also cover outright transfers: whether 'secured transactions' include such transfers will depend on domestic secured transactions law. For example, the UNCITRAL Model Law on Secured Transactions and some domestic secured transactions laws apply to outright transfers of receivables. The Geneva Securities Convention covers collateral transactions that are created by the grant of an interest in intermediated securities in the form of security interests and title transfer collateral agreements. Some domestic laws provide for fiduciary transfers of ownership that transfer 'ownership' of the asset to the creditor with the sole purpose of securing an obligation. Outright transfers of digital assets may be used in various contexts. It is therefore important that secured transactions law should be coordinated with a State's generally applicable rules governing outright transfers of digital assets. Another example of where domestic laws may differ relates to whether making a security right effective against third parties is seen as separate from creating a security right. In jurisdictions where some security rights are effective against third parties from the moment they are created, references in these Principles to making a security right effective against third parties should be read as references to the creation of a security right (see also Commentary 14.8).

14.4. In adopting these Principles, a State may need to amend existing secured transactions legislation by including special rules for digital assets as set out in Section V. In doing so, the digital asset to which these special rules apply will have to be defined, using the definition in Principle 2(2). For example, under the UNCITRAL Model Law on Secured Transactions (or any similar domestic secured transactions law) this would have the effect of carving out digital assets from the broader body of 'intangible assets' to which the generally applicable rules already apply (*e.g.*, third-party effectiveness by registration only). This would complement any existing definitions of special types of assets (*e.g.*, deposit accounts) for which asset-specific rules might have been provided (*e.g.*, third-party effectiveness may be achieved by control). Where a digital asset is linked to another asset ('the other asset'), that other asset may well fall within a specific category in the domestic law of a State, such as a category of 'securities' (bearing in mind that the existence and legal effect of the link is a matter for other law, see Principle 4). The nature of the link itself may, as a matter of other law, result in the linked digital asset falling within a specific category, such as that of negotiable documents or instruments (see Commentary 4.22). In these situations, the secured transactions rules specific to that category of asset will apply to the other asset or to the digital asset itself as appropriate.

14.5. States should consider providing for rules specific to digital assets. These rules may be made applicable to digital assets as a type of collateral or further distinctive rules could apply to various categories of linked digital assets. States should not attempt to provide for secured transactions rules specific to each of many categories of linked digital assets that would result in a complicated system. The concept of control set out in Principle 6 should apply equally to the third-party effectiveness of security rights in all types of digital assets (linked and non-linked) (see Principle 15).

14.6. The Principles in Section V address certain aspects of third-party effectiveness, priority and enforcement relating to security rights over digital assets. There will be many aspects of secured transactions that are governed by other law (as defined in Principle 2(4)). The rules determining the law applicable to proprietary aspects of secured transactions are set out in Principle 5(1) (subject to Principle 5(5)).

14.7. ***Illustration 1.*** The secured transactions law of State X does not carve out digital assets from the broader category of intangible assets. Control is a recognised mechanism for making a security right effective against third parties but is available only for bank accounts and intermediated securities. A secured creditor who has control of a digital asset may thus need to register to make its security right effective against third parties. Upon implementation of these Principles, the registration would be a redundant step in terms of providing public notice to third parties as, in the situation described, the secured creditor would be in control of the digital asset (as defined in Principle 6) which would make the security right effective against third parties by control under Principle 15.

Principles 14(2) and 14(3)

14.8. Principles 14(2) and 14(3) reflect Principle 4 which provides that the existence of, requirements for and legal consequences of any link between a digital asset and another asset (either a real-world asset or a digital asset) are a matter for other law. If, for instance, a link between a digital and a real-world asset is recognised under other law as operating as a negotiable document, the creation and third-party effectiveness of a security right in the digital asset would extend to the real-world asset. If it were not so recognised, a security right would extend to the digital asset only. This approach is consistent with, for instance, Article 16 of the UNCITRAL Model Law on Secured Transactions that provides for the creation of a security right in a negotiable document that may extend to goods. However, it does not define a negotiable document, as this is not a matter of secured transactions law. Furthermore, Principles 14(2) and 14(3) follow the approach of Article 17 of the UNCITRAL Model Law on Secured Transactions under which a security right in an asset does not extend to an 'associated asset', so that, for example, a security right in intellectual property does not extend to a tangible asset with respect to which that intellectual property is used. Accordingly, if some other law does not establish a link between the two assets, the creation of a security right in one of the two assets would not affect the other asset. The opposite situation, where a security right is taken in a real-world asset that is purported to be linked to a digital asset, is not covered by the Principles, because these Principles deal with digital assets only. As explained in Commentary 14.2, these Principles do not interfere

with domestic conceptions of security rights. In some jurisdictions, creation and third-party effectiveness are indistinguishable (see Commentary 14.3), in which case that State may not need to implement Principle 14(3).

14.9. ***Illustration 2.*** In State X, an invoice is not seen as an embodiment of the underlying right to payment. Factor A regularly takes control of digital invoices for due diligence purposes. This would not create a security right in the receivable nor make it effective against third parties. Factor B regularly takes a security right over receivables owed under invoices which are issued in the form of digital assets. The security right is made effective against third parties. This would not create a security right in the digital assets, *i.e.*, digital invoices, nor make it effective against third parties. Thus, in practice, because there is no effective link between the receivable and invoice, a security right over the digital invoice would not have any value in a similar way to a security right in a paper-invoice that does not embody a right to payment.

Principle 15

Control as a method of achieving third-party effectiveness

A security right in a digital asset can be made effective against third parties by control of the digital asset if one of the following requirements is fulfilled:

(a) the secured creditor has control of the digital asset as defined in Principle 6; or

(b) a custodian maintains the digital asset for the secured creditor as set out in Principle 10(2).

Commentary

Reasons for control as a method of third-party effectiveness

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

15.2. While in many States registration would generally render a security right in most (or all) types of assets effective against third parties (*e.g.*, in all movable assets covered by the UNCITRAL Model Law on Secured Transactions), registrations are not commonly effectuated in the crypto-lending market, leaving some credit risk in the transaction. Furthermore, in States that do not have a registration system for security rights, market participants may not be aware of the

existing requirements for third-party effectiveness or such requirements may be an obstacle to market practices.

15.3. 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 of the secured creditor, or by placing it under the control of the secured creditor (*e.g.*, in a multi-signature arrangement). Under some laws those steps may already be recognised as a method to make the security right in the digital asset effective against third parties. A transfer to a wallet held by the secured creditor or its agent would then be sufficient to protect the security right against third-party claims, including in the case of the insolvency of the borrower. Since these Principles do not interfere with the domestic conception of security rights, the protection in insolvency may be conferred by recognising the third-party effectiveness and priority, or excluding the digital asset from the estate of the debtor because it has been transferred to the secured creditor outright. Under laws that do not recognise such steps, the failure to register may be fatal for the secured creditor. In any case, the existing requirements for third-party effectiveness may create uncertainty for those who take digital assets as collateral.

15.4. Secured transactions and related laws may already provide for change of control over an asset to be sufficient to transfer it, whether outright or by way of security. Where laws already recognise some form of control over specified types of movable assets, security rights in digital assets that would fall under that type of a movable asset could be made effective against third parties by that form of control. For example, this might be the case of digital assets linked to securities held with securities intermediaries, depending on the effect of the link under other law. However, there are likely to be many other types of digital assets for which control mechanisms have not been provided in secured transactions laws.

15.5. In the past, regimes governing security rights in certain types of assets have been amended to reflect the emerging industry practice (*e.g.*, book entries to securities accounts in which financial collateral is held). As mentioned in Commentary 15.3, the prevailing practices in 'crypto-lending' do not rely on registration and other traditional methods of achieving third-party effectiveness.

Control as a method of third-party effectiveness

15.6. A State should refer to the definition of control in Principle 6 elsewhere in its law relating to digital assets and, if not, include the definition of control in Principle 6 in its secured transactions law as a means to achieve third-party effectiveness of a security right in a digital asset. Control within this definition exists when a secured creditor acquires a set of abilities with respect to the digital asset. Principle 15 (in conjunction with Principle 6(3) and Principle 10(2)) provides that the secured creditor may exercise the requisite abilities directly, through a third-party custodian or in cooperation with other parties, such as in a multi-sig arrangement (see Commentary 6.13). Incorporation of control in the law of a State as a means of third-party effectiveness of a security right will affect the structure of its priority rules, which is explored below in Principle 16 on priority, and facilitate enforcement, which is explored in Principle 17.

15.7. Recognition of control in a secured transactions law consistent with Principle 15 could result in a situation where the applicable law provides for multiple methods of third-party effectiveness. If a digital asset falls under a type of asset for which the secured transactions law has provided one or more methods to achieve third-party effectiveness, a security right may be made effective against third parties by any one of those methods. Principle 15 does not preclude a State from designating control as the sole method of third-party effectiveness with respect to security rights in digital assets, consistently with its general secured transactions law (*e.g.*, the law of a State may provide for control as the sole method of third-party effectiveness with respect to security rights in deposit accounts).

15.8. There are three situations in which control under these Principles may be used to make the security right effective against third parties. First, the secured creditor may acquire the requisite abilities prescribed in Principle 6. Second, the secured creditor may share these abilities with other parties, which would also constitute control under Principle 6 (see further Commentary 6.11). Third, a party that is currently in control (*e.g.*, a custodian) may agree to exercise the relevant abilities on behalf of the secured creditor. A version of this third situation is where a custodian maintains a digital

asset for a client by entering into a custody agreement with a sub-custodian (see Principle 10(2)).

Control shared by secured creditor and debtor

15.9. Commentary 15.9 to 15.13 addresses the situation where the secured creditor and the debtor share the abilities in Principle 6(1)(a) (this falls within the second situation referred to in Commentary 15.8). Principle 6(3) allows these abilities to be shared by multiple parties without compromising the existence of control. However, a person may have these factual abilities but, as a result of an agreement, that person's right to exercise one or more of those abilities may be legally restricted.

15.10. For some (non-digital) assets, other law may already recognise a degree of sharing of the right to dispose of the asset between the secured creditor and grantor without compromising the security right's effectiveness against third parties by control. This may vary from State to State. For instance, a security right in a bank account may be effective against third parties but the control agreement may enable the grantor to dispose of the asset until the secured creditor instructs the depository institution not to honour instructions from the grantor.

15.11. Principle 15 recommends that States design their rule on third-party effectiveness based on the sharing of factual abilities to align with Principle 6. Restrictions on the secured creditor's right to exercise the factual abilities will prevent the secured creditor's control being sufficient for effectiveness against third parties. Examples of such restrictions are where the secured creditor cannot, as a matter of fact, dispose of the digital asset and where the secured creditor is not permitted, by agreement, to dispose of the digital asset without the debtor's consent.

15.12. A State may wish to apply the approach to the third-party effectiveness of security rights with respect to other assets (see Commentary 15.10) to digital assets as well. If so, it may be sufficient in some States for the secured creditor to be in a position to exercise control when the debtor defaults, with the debtor retaining the right to exercise the factual abilities until that point. However, other States

may require, for third-party effectiveness, that the debtor has no right to exercise the factual abilities. This is a policy choice of the State.

Illustrations of control

15.13. ***Illustration 1.*** In State A, which has not adopted the Principles, a secured creditor takes a non-possessory pledge over a portfolio of digital assets. The applicable law does not provide a specific mechanism to make a security right effective against third parties with respect to digital assets but provides that registration is the sole mechanism to achieve third-party effectiveness over any intangible assets provided as collateral. The secured creditor has required its borrower to transfer the relevant digital asset to a third-party wallet controlled by the secured creditor through a multi-signature arrangement but does not make a registration. Later, the borrower enters into an insolvency-related proceeding. The secured creditor could lose its security right as it was not made effective against third parties in accordance with the law of State A. On the other hand, in State B which has adopted the Principles into its law, the secured creditor could have made its security right effective on the borrower's insolvency by control.

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

Principle 16

Priority of security rights

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

Commentary

Priority of secured creditor with control

16.1. Principle 16 addresses the situation where one secured creditor has made its security right in a digital asset effective against third parties by registration or another method recognised by the applicable law, but has not obtained control of the digital asset, and another secured creditor has made its security right in the same digital asset effective by control (pursuant to Principle 15). In this situation, Principle 16 provides that the latter would have priority even if it took the steps to obtain control after the former made its registration or otherwise made its security right effective against third parties. This is in contrast to the general rule (under the UNCITRAL Model Law on Secured Transactions and in many States), which is that the priority among competing security rights in the same asset is determined based on the temporal order of when the security right was made effective against third parties (typically, the order of registration). However, the law may grant priority to security rights in certain encumbered assets that are made effective against third parties by using a specific method for obtaining third-party effectiveness. For example, a security right in a negotiable instrument that has been made effective against third parties by possession typically has priority over other security rights made effective against third parties by other means. Similarly, the law of a State may recognise asset-specific priority rules for bank accounts, intermediated and non-intermediated securities, money, negotiable documents, and other types of assets.

16.2. This approach, applied to digital assets by Principle 16, may be justified in a number of ways. First, providing for the non-temporal priority recognises that the secured creditor that took the additional steps was relying to a greater extent on the encumbered asset. This is similar to a situation where a secured creditor takes possession of a negotiable document, which would give it priority over a security right made effective against third parties by registration, under some domestic regimes. Second, the secured creditor who made its security right effective against third parties by control would not need to search the registry. Again, this is similar to the position in relation to other assets, such as negotiable instruments, in that a party taking possession is not expected to search a registry, which reduces the cost of dealing with the asset and enhances its negotiability. Moreover, it is often not practical for a secured creditor taking security over a digital asset to search the registry. For transactions with digital assets, the prospective secured creditor might not even know which registry to search as the transferor, or its identity or its location, might be unknown. Third, this priority approach also reflects the lending practice ('margin lending') where creditors may extend credit to their clients to enable them to acquire a digital asset with respect to which they expect to have priority over an earlier-in-time registration. Fourth, it aligns the priority position with the position on default, when the secured creditor in control is best placed to enforce the security right, and provides an incentive for secured creditors to place themselves in this favourable position. By giving a secured creditor the ability to obtain priority, the rule contributes to market certainty. Moreover, the approach in Principle 16 is consistent with the secured transactions rules in international instruments, including the UNCITRAL Model Law on Secured Transactions and the relevant provisions of the Geneva Securities Convention, that give priority to secured creditors that acquired some form of control over the collateral.

16.3. In most States, other law has conferred some degree of transferability, typically negotiability, on some assets that allows transferees to cut off security rights made effective against third parties by registration or other means. For instance, a transferee of money takes free of a security right if it takes possession of money without knowledge that it violates the rights of a secured creditor. A transferee is defined in these Principles to include a secured creditor

(see Principle 2(5)). Since these Principles confer a high degree of negotiability on digital assets, their transferees (including secured creditors, see Principle 2(5)) will be able to benefit from the same approach, set out in Principle 8. Most secured creditors would be expected to satisfy the requirements of the innocent acquisition principle, including acting in good faith, without any disqualifying knowledge and extending value that a State may impose in accordance with Principle 8(1)(b). This is particularly true because, as described above, a secured creditor that makes its security right effective against third parties by control will not be expected to search any secured transactions registry. While under Principle 8 a secured creditor may qualify as an innocent acquirer only if it acts without knowledge of a competing interest, the effect of Principle 16 is that the secured creditor that takes control would have priority over one that registers irrespective of knowledge. The same result would be achieved under many secured transactions laws, including the UNCITRAL Model Law on Secured Transactions (see Article 45) which provides that knowledge of a competing security right does not affect the priority of a security right.

Control by more than one secured creditor

16.4. More than one secured creditor can obtain control (or share the relevant abilities) over the digital assets, which includes making their security right effective against third parties. This situation may arise where the digital asset is held by a custodian who agrees to maintain the digital asset for multiple secured creditors. Generally, the two creditors would be expected to regulate their respective priority in a subordination or inter-creditor agreement. In the absence of an agreement, the priority conflict may be determined based on the general priority rule contained in the applicable secured transactions law, which would typically reflect the first-in-time principle, *i.e.*, the secured creditor who was the first to obtain an acknowledgment of the custodian would have priority.

Applicable law

16.5. Principle 5(1) determines the law applicable to a conflict between a security right made effective against third parties by control and a competing security right made effective against third parties by

means other than control, such as registration. As specified in Principle 5(5)(b), other law determines the law applicable to a conflict between security rights made effective against third parties by a method other than control. For instance, under the UNCITRAL Model Law on Secured Transactions the law applicable to the priority of a security right in an intangible asset is the law of the grantor's location. This priority conflict is not addressed in this Principle, and is a matter of general secured transactions law.

16.6. ***Illustration.*** A security right in all the assets of the borrower is made effective against third parties by registration. Upon disposal of encumbered inventory by exchanging it for digital assets, those digital assets are collected by the borrower and deposited with a custodian that has control over the digital assets. The custodian extends a loan to the borrower that is secured with all digital assets under its control. The security right of the custodian has priority over the security right in the digital assets claimed as proceeds of the inventory, assuming that the secured transactions law recognises control as a method of obtaining effectiveness against third parties (see Principle 15), and gives priority to a security right made effective against third parties by control (see Principle 16).

Principle 17

Enforcement of security rights

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

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

Commentary

General

17.1. Principle 17 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). These and other aspects regarding effective enforcement are explored in another project of UNIDROIT on 'Best Practices for Effective Enforcement'.

17.2. Principle 17 does not prescribe particular enforcement methods for security rights in digital assets. Generally available methods provided under other law would apply, including judicial enforcement. This Commentary provides guidance to States as to how existing enforcement rules, such as those included in Chapter VII of the UNCITRAL Model Law on Secured Transactions, should apply in relation to such security rights. The law of a State should not preclude secured creditors from exercising remedies that may exist under other laws or have been provided for in the security agreement. When digital assets become widely used in securities transactions, derivatives, and similar financial structures, States should ensure that close-out netting is available to parties to such transactions. As explained above in the Commentary to Principle 14, these Principles

do not recommend changes to the characterisation of secured transactions under the applicable law. In some cases in the enforcement of rights, thus, the applicable other law may impose no, or lower, requirements on secured creditors that have acquired a digital asset outright.

17.3. All enforcement actions, including disposal, collection of payment (if the right to payment of a monetary obligation is the asset to which a digital asset is effectively linked) and acceptance of the collateral, in full or partial satisfaction of the secured obligation, should be available in relation to security rights in digital assets. In enforcing their rights, secured creditors must proceed in accordance with the applicable enforcement rules contained in a general secured transactions law, including, for example, requirements to proceed in a commercially reasonable manner, provide notifications, distribute any proceeds in accordance with the priority rules, etc. In some cases, the inherent design of the digital asset may prevent the exercise of certain enforcement rights. General rules governing enforcement of security rights included in international standards on secured transactions appear to be flexible enough to accommodate the expectation of digital assets lenders and other relevant parties. However, States should take into account a number of considerations, which are set out in Commentary 17.4 to 17.7.

17.4. The method used to make the security right effective against third parties can have an impact on the ability to enforce security rights. Control is a facilitator of enforcement upon default, so that if a security right is made effective against third parties by control, enforcement by the secured creditor is likely to be reasonably straightforward. However, if a security right in a digital asset is made effective against third parties by registration rather than by control, it is likely to be difficult in practice for the secured creditor to enforce against that asset without the cooperation of the grantor, since the grantor retains control of the asset. Thus, the secured creditor might need to obtain a court order, after default, to obtain control if the grantor refuses to transfer it. This situation would be analogous to the grantor refusing to surrender possession of a tangible asset. Furthermore, control might have been transferred to another secured creditor who would have priority (see Principle 16). The general enforcement rules of the secured transactions law then determine

whether and how a senior secured creditor may take over the enforcement process.

17.5. Secured transactions laws typically balance the interests of affected parties by imposing certain requirements on secured creditors when enforcing a security right, such as to provide notifications to affected parties. However, secured transactions laws may also provide that under certain situations these requirements will not apply. For instance, Article 78(8) of the UNCITRAL Model Law on Secured Transactions provides for exceptions from the requirement to provide a notification when the asset may speedily decline in value or is sold on a recognised market. These kinds of exceptions would, arguably, apply to many, though not all, digital assets (*e.g.*, bitcoin may speedily decline in value while stable coins may not, and some NFTs may already trade on recognised markets while others do not). Enforcement provisions in secured transactions laws may not need to be changed to accommodate digital assets if these exceptions are crafted broadly to accommodate future developments. Some States also have bespoke enforcement procedures for specific types of assets which do not include any notification requirements (for example, in relation to intermediated securities, Article 33 of the Geneva Securities Convention provides for enforcement by sale or appropriation of securities without notice). It would be consistent with Principle 17 for a State to provide for an analogous enforcement procedure in relation to security rights over digital assets, particularly those which are similar to the types of assets for which such enforcement procedures already exist.

17.6. The recognition of exceptions from the generally applicable enforcement provisions facilitates automated enforcement. An example of automatic enforcement is where liquidation of a digital asset occurs automatically when the collateral-to-loan ratio falls under a specified threshold. This would be an enforcement of a security right if the fall in the ratio is a default under the terms of the security agreement. Many system designers are not aware of how the secured transactions enforcement rules apply. Even if systems have been designed to fit within any exceptions from the general enforcement provisions, the secured creditor would still need to proceed in a commercially reasonable manner or in conformity with some other applicable standard, such as good faith.

17.7. Courts may need some guidance on the interpretation of any exceptions to the enforcement requirement when it comes to digital assets. For instance, in relation to one of the exceptions mentioned in Commentary 17.5, a 'recognised market' is one in which the items sold are fungible and prices are not subject to individual negotiation, such as stock or commodity exchanges. The intended goals of the recognised market exceptions is to facilitate the efficiencies and cost savings that the special treatment may provide without disadvantaging affected parties. Although a recognised market need not be subject to regulation or supervision, the existence of regulatory requirements or guidelines may provide useful guidance for applying this exception. The test of whether or not the market would qualify for the exception is a functional one. It is not based on the 'type' of market. These are some of the parameters that would determine whether an exchange for digital assets actually qualifies as a recognised market.

Principle 17(2)

17.8. If a custodian maintains the digital asset for the grantor, extra-judicial enforcement will entail action by that custodian on the instructions of the secured creditor. An intermediary will be unwilling to follow those instructions if the secured creditor is unknown, and many secured transactions laws include provisions protecting intermediaries in this situation. For example, Article 82(4) of the UNCITRAL Model Law on Secured Transactions provides that, in relation to a security right over a bank account, extra-judicial enforcement is only available when the bank has agreed to act on the instructions of the secured creditor. Principle 17(2) provides for the protection of custodians of digital assets in the enforcement of a security right. If the security right has been made effective against third parties by control under Principle 15, the custodian would maintain the digital asset for the secured creditor, and would typically owe some duties to that secured creditor, including to change the control of the digital assets if instructed by the secured creditor (see Principle 11(1)(b)). In contrast, if the security right has been made effective by a method other than control, such as by registration, the custodian would not owe any duties to that secured creditor. In those situations, the secured creditor will need to obtain an order from a court or other public authority, if the custodian does not agree to act on the instructions of the secured creditor.

17.9. ***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. An action of two parties is required to cause a change of control. Upon default, the multi-signature arrangement is triggered, and the encumbered digital asset is transferred under the 'sole' control of the secured creditor resulting in the acceptance of the collateral in satisfaction of the secured obligation or enabling a foreclosure sale. However, any requirements under the applicable other law as to acceptance of the collateral in satisfaction of the obligation would continue to apply.

SECTION VI: PROCEDURAL LAW INCLUDING ENFORCEMENT

Principle 18

Procedural law including enforcement

Unless otherwise provided for in these Principles, other law applies in respect of procedural matters, including enforcement, relating to digital assets.

Commentary

18.1. Principle 18 makes it clear that the ordinary procedural law of a State, will apply to (i) any court proceedings concerning non-enforcement matters involving digital assets, (ii) any procedures for the enforcement of court orders involving digital assets, or (iii) execution by way of authority with respect to digital assets. The first category includes proceedings which are not enforcement proceedings: such proceedings would include priority contests and proceedings in which it was necessary for a person to prove that they had control of a digital asset (see Principle 7). Category (ii) is self-explanatory. What is meant by category (iii) is explained in the rest of this paragraph. Execution is the process through which a creditor can obtain satisfaction of its claim against an obligor, by reaching and applying the value of an asset of the obligor or by a public authority obtaining rights in, or control over, such an asset. Depending on the jurisdiction (and the situation), this process can be triggered by various means including a court judgment or court order, an enforceable arbitral award, an out-of-court settlement which is given effect by law other than the law of contract or by an authentic document such as a document issued by a notary or other public authority, or another enforceable instrument as defined by law. The process is carried out by a public authority or a private actor under the supervision of a public authority.

18.2. However, depending on the content of the procedural law of a particular State, some adaptations either to the law or the way the law operates in practice may be advisable in order to take account of

the distinctive features of digital assets. Commentary 18.3 to 18.7 set out some examples of features, or combinations of features, which might make adaptations advisable.

18.3. In order to enforce a court order involving digital assets, or execution by way of authority with respect to digital assets, it will often be necessary for a public authority or a person authorised by a public authority to take control of one or more digital assets. This, however, may not be straightforward, compared to taking control (or taking possession) of other types of assets. For example, in a situation where the person who controls the digital asset is identified, that person might refuse to reveal the password which gives access to the wallet and/or the private key. It will therefore be necessary for a court (or other authority) to order that person to make a change of control or to otherwise enable access to the asset. It would be advisable for procedural law, and its operation, to facilitate this.

18.4. Where the identified person in control of the digital asset is a custodian, the public authority or person authorised by the public authority will want to instruct the custodian to make a change of control or to otherwise enable access to the asset. Again, unless the custodian agrees to do this, it would be necessary for a court (or other authority) to order the custodian to make a change of control or to otherwise enable access to the asset. It would be advisable for procedural law, and its operation, to facilitate this.

18.5. Another possible difficulty arising from the distinctive features of digital assets is that it will not always be straightforward to identify the person in control of the relevant digital asset. In this situation, the public authority, or person authorised by the public authority, may wish to obtain information from a third party, such as a custodian. For example, the information could be the information mentioned in Principle 6(1)(b). In other situations, information from a third party could be required more generally to enable proceedings or any process (such as an execution process) to be commenced or otherwise to be effective. In relation to all these situations, it would be advisable for procedural law, and its operation, to facilitate the necessary information to be obtained, although a balance will need to be struck between this facilitation, on one hand, and confidentiality and privacy requirements, on the other.

18.6. One feature of digital assets is that they can be transferred easily and quickly. In some situations, even though a tracing claim against substitute assets may remain (depending on the applicable other law), the value represented can be lost. Therefore, asset preservation could be important in court or other proceedings or in an execution process. It would be advisable for procedural law to facilitate this, for example, by providing for interim relief such as a freezing order or an order that control of digital assets be transferred to the court or other public authority.

18.7. A further feature of digital assets and the systems on which they are recorded is that they have no physical situs and the people who control them from time to time may be in many different jurisdictions. As a result, proceedings or execution processes are likely to be cross-border and involve courts or public authorities in many different jurisdictions. It would therefore be advisable for procedural law to take this into account.

18.8. Detailed work on the subject of execution by way of authority in respect of digital assets is being carried out by the UNIDROIT project on 'Best Practices for Effective Enforcement' and for specific guidance, reference is made to the future work of this project.

SECTION VII: INSOLVENCY

Principle 19

Effect of insolvency on proprietary rights in digital assets

(1) A proprietary right in a digital asset that has become effective against third parties under Principles law or other law is effective against the insolvency representative, creditors, and any other third party in an insolvency-related proceeding.

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

(a) the ranking of categories of claims;

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

(c) the enforcement of rights to an asset that is under the control or supervision of the insolvency representative.

Commentary

General

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

19.2. Apart from situations falling within the innocent acquisition rule in Principle 8 and the rule in Principle 15 whereby a security right can be made effective against third parties by control, Principle 3(3) establishes that whether a person has a proprietary right in a digital asset and whether a proprietary right in a digital asset has been made effective against third parties is a matter of 'other law' (that is, any part of the law of a State that is not Principles law (Principle 2(4)). Principle 19(1) provides for the pre-insolvency effectiveness to continue in an insolvency-related proceeding: the precise result of that effectiveness will also depend on the circumstances and on the applicable other law. In general, however, as recommended in part two of the UNCITRAL Legislative Guide on Insolvency Law (2004) (see recommendation 35), the debtor's estate will comprise assets of the debtor, which are those in which the debtor has a proprietary right, to the extent of that proprietary right.

Typical situations

19.3. The consequences of the operation of Principle 19 can be illustrated by considering three typical situations. (1) The insolvency of a person who 'owns' a digital asset, or who, as a secured creditor, has acquired a security right in a digital asset, (2) the insolvency of a person, who, as a debtor, has granted to its creditor a security right in a digital asset as collateral, and (3) the insolvency of a custodian, who controls a digital asset for a client. The client will wish to retrieve its digital asset. Principle 19 primarily concerns situations (1) and (2), which are considered in Commentary 19.4 to 19.8, which, by way of example, illustrate the operation of Principle 19 in the context of an insolvency-related proceeding resulting in a distribution to creditors. Situation (3) (insolvency of a custodian) is considered specifically in Principle 13 and the Commentary to that Principle. Insolvency of a sub-custodian is covered by Principle 13(8).

Situation (1)

19.4. Situation (1) can arise in a number of variations. In the first variation of situation (1) a person owns and controls a digital asset, for example, by using wallet software as a form of 'self-custody' (see Commentary 10.15 to 10.17). When this person becomes insolvent, the digital asset forms part of that person's estate, since the person's

proprietary right remains effective on insolvency (Principle 19(1)). Under typical insolvency law, the insolvency representative can infringe upon an insolvent person's proprietary rights in that they can exercise an insolvent person's proprietary rights for the benefit of that insolvent person's creditors. Thus, the insolvency representative may assume control over the insolvent person's digital assets, sell those assets and distribute the proceeds amongst the creditors. Notably, 'control' here is used in a broad sense, and not as defined in Principle 6. Therefore, in situation (1), the insolvency representative is likely to want to retrieve the digital asset, and sell it for the benefit of the insolvent person's creditors. Taking control of the digital asset, however, may not be straightforward, compared to taking control of other types of assets. Access to the wallet and/or the private key is likely to be passworded, and the insolvent person might refuse to reveal the password. Whether (and how) the insolvency representative can obtain a court order against the insolvent person ordering him to reveal the password will depend on the applicable insolvency law.

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

19.6. The third variation of situation (1) concerns the situation where a person becomes insolvent who, as a secured creditor, has acquired a security right in a digital asset. To make her security right effective, this person may have obtained control of the relevant digital asset, or may have made her security right effective by other methods available under the applicable law (see also Principle 16 and the Commentary to that Principle). Both instances are similar to the first variation, in that both in the first and in this third variation, the insolvent person has a proprietary right (as 'owner' or as secured creditor, respectively) in the digital asset. When the secured creditor becomes insolvent, the security right in the digital asset forms part of

that person's estate, since the person's proprietary right remains effective on insolvency. See further Commentary 19.4.

19.7. The fourth variation of situation (1) is where the insolvent person acquired, as a secured creditor, a security right in the digital asset but the asset is maintained for her by a custodian. This variation is similar to the second variation. The insolvent creditor's security right remains effective despite the insolvency-related proceeding. See further Commentary 19.5.

Situation (2)

19.8. There are also a number of variations of situation (2). In the first variation, a person owns and controls a digital asset in some sort of self-custody arrangement (see Commentary 10.15 to 10.17) and that person has granted a security right in the digital asset to his creditor. On that person's insolvency, the creditor may wish to enforce the security right in the digital asset during the debtor's insolvency. Under Principle 19(1) the creditor's security right is not affected by the insolvency. This means that (depending on the applicable insolvency law and concrete situation) the security right can be enforced by the creditor or the insolvency representative can realise the value of the asset and pay the creditor out of this value. In any event, the creditor's security right will have the same effect as a security right in any other asset (which will depend on the applicable insolvency law, see, for example, Commentary 19.12), but the same possible difficulties about obtaining control of the asset mentioned above will occur. The same analysis applies if the digital asset is maintained by a custodian for the insolvent person, except that unless the custodian has agreed to act on the instructions of the secured creditor, an order from a court or other authority will be required (see Principle 17(2)). If the secured creditor has taken control of the digital asset, it is much easier for it to enforce the security right extra-judicially (see Commentary 17.4), but whether it can do so will depend on the applicable insolvency law.

Principle 19(2)

19.9. While Principle 19 is meant to leave a person's proprietary rights in a digital asset unaffected by insolvency, this protection is not

absolute (see also Principles 5(6) and 5(7)) For example, the application of the other law of a State may result in the preference of another person's rights over the relevant digital asset. Principle 19(1) does not affect the operation of such a rule, whether it is substantive or procedural, providing that it applies by virtue of the insolvency-related proceeding. These rules may be found in any part of the law of a State that is not Principles law (*i.e.*, that is 'other law' as defined in Principle 2(4)), including its tax law, insolvency law, general private law, and its procedural law. Principle 19(2) lists three examples of instances where the relevant rules of the other law of a State may affect the rights of creditors, which are not affected by Principle 19(1).

19.10. The first example, set out in Principle 19(2)(a), concerns the ranking of categories of claims. An applicable State's law governing the priority order in which claims on the insolvent estate or on specific assets forming part of the estate are to be ranked, will typically dictate that certain categories of creditors have preference over other creditors (including secured creditors). For example, the law of a State may prescribe that fiscal authorities have priority over secured and unsecured creditors in relation to certain assets of the insolvent person, or that the costs of the insolvency-related proceeding have preferential status over other secured and unsecured creditors' claims on the insolvent estate.

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

19.12. The third example, set out in Principle 19(2)(c), clarifies that, if the insolvency representative has taken 'control' of the digital asset as described in Commentary 19.4, Principle 19(1) does not affect the

operation of any rule of the applicable law relating to the enforcement of rights to that asset whether by the insolvency representative or anyone else. For example, a rule providing for a stay on enforcement by a secured creditor would not be affected by Principle 19(1). Principle 19(2)(c), read in conjunction with Principle 19(1), therefore also implies that third parties, including the system that operates the (record of the) digital assets in question, must acknowledge and accommodate the insolvency representative's exercise of the insolvent person's rights in these digital assets. For custody situations, see Principle 13.

WORKING GROUP
FOR THE PREPARATION OF THE
PRINCIPLES ON DIGITAL ASSETS AND PRIVATE LAW

MEMBERS

Hideki KANDA — Professor of Law, Gakushuin University, Japan; *Member of the UNIDROIT Governing Council*, *Chair of the Working Group*

Louise GULLIFER — Rouse Ball Professor of English Law, University of Cambridge, United Kingdom; *Chair of the Drafting Committee*, *Co-Chair of the Subgroup on Holding and Custody*

Jason Grant ALLEN — Associate Professor of Law, SMU Yong Pung How School of Law, Singapore (former Senior Research Fellow, Humboldt University of Berlin, Germany), Australia

Reghard BRITS — Attorney & Conveyancer, Brits Dreyer Inc., South Africa

Marek DUBOVEC — Professor of Practice, James E. Rogers College of Law, University of Arizona, United States of America; *Member of the Drafting Committee*, *Chair of the Subgroup on Secured Transactions*

David FOX — Professor of Common Law, Edinburgh Law School, University of Edinburgh, United Kingdom; *Member of the Drafting Committee*

Matthias HAENTJENS — Professor of Civil Law, Leiden University, Netherlands; *Member of the Drafting Committee, Co-Chair of the Subgroup on Transfer*

Hannah Yee-Fen LIM — Associate Professor in Business Law, Nanyang Technological University, Singapore

Hin LIU — Law Lecturer, University of Oxford, United Kingdom and Hong Kong

Charles W. MOONEY Jr. — Professor of Law, University of Pennsylvania, United States of America; *Member of the Drafting Committee*, *Co-Chair of the Subgroup on Transfer*

Philipp PAECH — Associate Professor of Law, London School of Economics & Political Science, United Kingdom and Germany; *Member of the Drafting Committee*, *Chair of the Subgroup on Conflict of Laws*

Carla REYES — Associate Professor of Law (former Assistant Professor of Law), SMU Dedman School of Law, United States of America

Nina-Luisa SIEDLER — Partner, Möhrle Happ Luther (former Partner, DWF), Germany

Luc THEVENOZ — Professor of Law, Université de Genève, Switzerland; *Member of the Drafting Committee*, *Co-Chair of the Subgroup on Holding and Custody*

Hubert de VAUPLANE — Partner, Kramer Levin Naftalis & Frankel LLP; Professor of International Banking and Financial Law, Paris Institute for Political Sciences, France

Jeffrey WOOL — Secretary-General, Aviation Working Group, United States of America[3]

UNIDROIT SECRETARIAT

Ignacio TIRADO — Secretary-General

Anna VENEZIANO — Deputy Secretary-General

Hamza HAMEED — Legal Consultant

Carlo DI NICOLA — Senior Legal Officer

Theodora KOSTOULA — Legal Consultant

MIAO Chen — Legal Officer in secondment

Michelle FUNG — Legal Officer in secondment

Hossein NABILOU — UNIDROIT-Bank of Italy Chair Programme

[3] ZOU Mimi (Visiting Fellow, Oxford Martin School, University of Oxford, China) also participated in the first stages of the project.

INSTITUTIONAL OBSERVERS

AUSTRALIAN ATTORNEY GENERAL'S DEPARTMENT

Brody WARREN — Assistant Director, Private International and Commercial Law Section, Australia

Alistair DUNBAR — Legal Policy Advisor, Private International and Commercial Law Section, Australia

AUSTRALIAN FINANCIAL SECURITY AUTHORITY

Gavin MCCOSKER — Deputy Chief Executive, Australia

BANCA D'ITALIA (CENTRAL BANK OF ITALY)

Nicola DE GIORGI — Senior Lawyer, Italy

Vincenza PROFETA — Senior Lawyer, Italy

BUSINESS REGISTRATION SERVICE (GOVERNMENT OF KENYA)

Shighadi MWAKIO — Deputy Registrar MPSR, Kenya

COMMISSIONE NAZIONALE PER LE SOCIETÀ E LA BORSA (CONSOB)

Martina TAMBUCCI — Head of International Relations Office, Italy

Nicolò BRUGIOLO — International Relations Office, Italy

Virna COLANTUONI — International Relations Office, Italy

Raffaella PANTANO — International Relations Office, Italy

Maria Tecla RODI — International Relations Office, Italy

EUROPEAN BANKING AUTHORITY (EBA)

Elisabeth NOBLE — Senior Policy Advisor, Banking Markets, Innovation and Products, France; *Member of the Drafting Committee*

HAGUE CONFERENCE ON PRIVATE INTERNATIONAL LAW (HCCH)

Gérardine GOH ESCOLAR — Deputy Secretary General (former First Secretary), Permanent Bureau, Netherlands

INTERNATIONAL MONETARY FUND (IMF)

Marianne BECHARA — Senior Fintech Legal Counsel, United States of America

ISTITUTO PER LA VIGILANZA SULLE ASSICURAZIONI (IVASS)

Antonella ALTOMONTE — Lawyer, Italy

Simone CASTROVINCI ZENNA — Lawyer, Italy

LAW COMMISSION OF ENGLAND AND WALES

Sarah GREEN — Law Commissioner for Commercial and Common Law, United Kingdom

Matthew KIMBER — Lawyer, Commercial and Common Law, United Kingdom

Amila KULASINGHE — Lawyer, Commercial and Common Law, United Kingdom

Síona MOLONY — Research Assistant, United Kingdom and Ireland

MINISTRY OF COMMERCE OF THE PEOPLE'S REPUBLIC OF CHINA

LIU Keyi — Deputy Director, Domestic Trade Law Divisions, Treaty & Law Department, China

MINISTRY OF FINANCE OF THE CZECH REPUBLIC

Alex IVANČO — Director, Financial Markets III Department, Czech Republic

UNIFORM LAW COMMISSION

Andrea TOSATO — Associate Professor of Commercial Law, University of Nottingham, United Kingdom; Visiting Associate Professor in Law, University of Pennsylvania, United States of America; *Member of the Drafting Committee*

UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAW (UNCITRAL)

Jae Sung LEE — Senior Legal Officer, Austria

Samira MUSAYEVA — Senior Legal Officer, Austria

Luca CASTELLANI — Legal Officer, Austria

Benjamin HERISSET — Legal Officer, Austria

Alexander KUNZELMANN — Legal Officer, Austria

Thomas TRASCHLER — Legal Officer, Austria

WORLD BANK GROUP

GYNEDI Srinivas — Senior Financial Sector Specialist, Payment Systems Development Group, Finance, Competitiveness & Innovation, United States of America

Working Group

AMERICAN LAW INSTITUTE (ALI)

Steven WEISE — Life Member, ALI Council; Partner, Proskauer Rose LLP, United States of America; *Member of the Drafting Committee*

ASOCIACIÓN AMERICANA DE DERECHO INTERNACIONAL PRIVADO (ASADIP)

Luis Ernesto RODRÍGUEZ CARRERA — Secretary General, Venezuela

ASSOCIATION INTERNATIONALE DES SCIENCES JURIDIQUES / INTERNATIONAL ASSOCIATION OF LEGAL SCIENCE (AISJ/IALS)

J.H.M. Sjef VAN ERP — President, Netherlands

Agustin PARISE — Secretary-General, France

ASSOCIATION OF GLOBAL CUSTODIANS

John SIENA — Associate General Counsel and Co-Head of Regulatory Strategy, Brown Brothers Harriman, United Kingdom

EUROPEAN BANKING INSTITUTE (EBI)

Matthias LEHMANN — Professor of Private Law, Private International Law and Comparative Law, Universität Wien, Austria and Germany

EUROPEAN LAW INSTITUTE (ELI)

Pascal PICHONNAZ — President (ELI), Austria; Ordinary Professor, University of Fribourg, Switzerland

Christiane WENDEHORST — Scientific Director (ELI); Professor of Law and Co-Head of the Department of Innovation and Digitalisation in Law, University of Vienna, Austria

Phoebus ATHANASSIOU — Senior Lead Legal Counsel, (former Principal Legal Counsel), European Central Bank, Germany; Co-Drafter, ELI Principles on the Use of Digital Assets as Security

Teemu JUUTILAINEN — Associate Professor, University of Turku, Finland; Co-Drafter, ELI Principles on the Use of Digital Assets as Security

Teresa RODRÍGUEZ DE LAS HERAS BALLELL — Associate Professor of Commercial Law, Universidad Carlos III de Madrid, Spain

INTERNATIONAL BAR ASSOCIATION – BANKING LAW COMMITTEE (BLC)

Klaus LÖBER — Former Vice Chair (BLC), Germany

Fernando AZOFRA — Co-Chair (former Vice Chair) (BLC); Partner, Uría Menéndez, Madrid

Giorgio BOVENZI — Officer (BLC); Partner, Haynes and Boone LLP, United States of America and Italy

INTERNATIONAL LAW INSTITUTE

Bob TROJAN — Senior Advisor, United States of America

INTERNATIONAL SWAPS AND DERIVATIVES ASSOCIATION (ISDA)

Peter WERNER — Senior Counsel, United Kingdom

INTERNATIONAL UNION OF JUDICIAL OFFICERS (UIHJ)

Jos UITDEHAAG — First Vice-President, Netherlands

ITALIAN ASSOCIATION OF FINTECH & INSURTECH (ASSOFINTECH)

Alessandro M. LERRO — Chairman of the Scientific Committee, Italy

KOZOLCHYK NATIONAL LAW CENTER (NATLAW)

Ignacio DE LEON — Chief Executive Officer, United States of America

Spyridon V. BAZINAS — Lead Advisor, United States of America

X REALITY SAFETY INITIATIVE (XRSI)

Marco MAGNANO — Director of Communications, Italy

Elizabeth SHUBOV — Web3 & Blockchain Adviser, United States of America

INDIVIDUAL OBSERVERS

Sir Roy GOODE — Emeritus Professor of Law, St John's College, University of Oxford, United Kingdom

Jeremy BACHARACH — Associate, Lenz & Staeheli, Switzerland (former Visiting Researcher, Harvard Law School, United States of America)

France DRUMMOND — Professor, Université Paris II Panthéon-Assas; Director, Institut de Recherche en Droit des Affaires (IRDA Paris), France

Analía GÓMEZ BOHLE — Professor, Faculty of Law, Universidad de Buenos Aires, Argentina

Andrew M. HINKES — Partner, K&L Gates, United States of America

Zeynep Ülkü KAHVECI — Former UNIDROIT Scholar, Türkiye

Caroline KLEINER — Professor, Université de Paris, France

Giovanna MASSAROTTO — Research Fellow, Center for Technology, Innovation and Competition, University of Pennsylvania, United States of America and Italy

Camilla VILLARD DURAN — Associate Professor of Law, ESSCA School of Management, France (former Associate Professor, Universidade de São Paulo, Brazil)

Vincent YESUE — Associate Attorney, Rusing Lopez & Lizardi PLLC, United States of America

STEERING COMMITTEE

CHAIR

Monika PAUKNEROVÁ — Professor of Private International Law, Faculty of Law, Charles University, Czech Republic; *Member of the UNIDROIT Governing Council*

ARGENTINA

Alejandro LUPPINO — Counsellor, Embassy of the Argentine Republic in Italy, Rome

Sebastián PAREDES — Professor, Universidad de Buenos Aires, Buenos Aires

AUSTRIA

Verena CAP — Lead Prosecutor, Federal Ministry of Justice, Vienna

BELGIUM

Hervé JACQUEMIN — Professeur de droit économique, Directeur du Centre de Recherche Information, Droit et Société, Université de Namur, Namur

BRAZIL

Alexandre PINHEIRO DOS SANTOS — General Superintendent of the Securities and Exchange Commission of Brazil, Rio de Janeiro

Antonio Marcos FONTES GUIMARÃES — Head Division, Financial System Regulation Department, Central Bank of Brazil, Brasilia

CHILE

Ignacio GARCÍA — Professor of International Law, College of Law of the Pontificia Universidad Católica de Chile, Santiago

CHINA

GUO Yu — Associate Professor, School of Law, Peking University, Beijing

XIN Biqiu — Department of Treaty & Law, Ministry of Commerce, Beijing

CZECH REPUBLIC

Alex IVANČO — Director, Financial Market Supervision Department, Ministry of Finance, Prague

Zdeněk KUČERA — Partner, Head of TMT, Dentons; Head of Technology and Digitalization Center, Univerzita Karlova, Prague

FINLAND

Markus TERVONEN — Senior Advisor, Ministry of Justice, Helsinki

FRANCE

Juliette MONGIN — Maître des requêtes en service extraordinaire, Conseil d'État, Paris; ancienne Cheffe du bureau du droit des obligations de la direction des affaires civiles et du Sceau, Ministère de la Justice, Paris

GERMANY

Ute HÖHFELD — Head of Section for Law relating to Commercial Register, Cooperatives – Law relating to Securities, Federal Ministry of Justice and Consumer Protection, Berlin

HOLY SEE

Paolo PAPANTI-PELLETIER — Judge, Vatican City Tribunal, Vatican City

HUNGARY

Attila MENYHÁRD — Professor of Civil Law, Faculty of Law, Civil Law Department, Eötvös Loránd (ELTE) University, Budapest; *Member of the UNIDROIT Governing Council*

IRAN (ISLAMIC REPUBLIC OF)

Hamed HAGHBAYAN — Senior Legal Officer, Central Bank of Iran, Tehran

Reza JAVADINIA — Ministry of Industry, Mine and Trade, Tehran

Noorian DARIAN — Ministry of Commerce, E-Commerce Development Center, Tehran

Arghavan GHOBADI — Legal Department, Ministry of Foreign Affairs, Tehran

Mahdi JANATI MOHEB — Legal Expert, Ministry of Foreign Affairs, Tehran

ITALY

Rita CARACUZZO — Legal expert, Ministry of Foreign Affairs and International Cooperation, Rome

Giusella FINOCCHIARO — Full Professor of Private Law and Internet Law, University of Bologna, Bologna

JAPAN

MORISHITA Tetsuo — Professor, Sophia University Law School, Tokyo

LATVIA

Iveta GEDUS — Head of Division of International and Procedural Law, Civil Law Department, Ministry of Justice, Riga

LUXEMBOURG

Dirk Andreas ZETZSCHE — Professor in Financial Law, ADA Chair in Financial Law and Inclusive Finance, University of Luxembourg, Luxembourg

MEXICO

Luis Manuel MÉJAN CARRER — Law Professor, Instituto Tecnológico Autónomo de México, Mexico City

NETHERLANDS

T.F.E. (Eric) TJONG TJIN TAI — Full Professor of Private Law, Tilburg University, Tilburg

REPUBLIC OF KOREA

Jaemin CHOUNG — Legal Counsel, Ministry of Justice, Gyeonggi-do

RUSSIAN FEDERATION

Alexey V. MINAEV — Deputy Director, Department of Digital Trade, Ministry of Economic Development of Russia, Moscow

SERBIA

Jelena ĆERANIĆ PERIŠIC — Professor, Chair of the Scientific Council, Institute of Comparative Law, Belgrade

SPAIN

Manuel BAENA PEDROSA — Consular Affairs Officer, Embassy of Spain to Ukraine; former Counsellor, International Legal Department and Procedural Law Department of Civil Law, Ministry of Foreign Affairs, European Union and Cooperation (MAEUEC), Madrid

SWITZERLAND

Sonja MAIRE — Legal Officer, Federal Office of Justice, Bern

Corinne ZELLWEGER-GUTKNECHT — Professor of Private Law, University of Basel, Basel

TÜRKIYE

Işil Selen DENEMEÇ — Digital Transformation, Office of the Presidency of the Republic of Turkey, Legal Department, Ankara

Leyla KESER BERBER — Professor, IT Law Institute, Istanbul Bilgi University, Istanbul

Osman GAZİ GUCLUTURK — Senior Policy Associate, Holistic AI, London; former Assistant Professor of IT Law, Bogazici University, Istanbul

UNITED STATES OF AMERICA

Joseph KHAWAM — Attorney-Adviser, U.S. Department of State, Washington, D.C.

Edwin E. SMITH — Partner, Morgan, Lewis & Bockius LLP, Boston/New York

URUGUAY

Marcos DOTTA — Director, International Law Affairs, Ministry of Foreign Affairs, Montevideo

EUROPEAN COMMISSION

Angela SANGUINETTI — Directorate-General - Justice and Consumers (DG JUST), Brussels

Rok ZVELC — Directorate-General for Financial Stability, Financial Services and Capital Markets Union (DG FISMA), Brussels

THE UNIDROIT GOVERNING COUNCIL

(2019-2023)

Maria Chiara MALAGUTI	President of UNIDROIT
Stefania BARIATTI	Italy
Hans-Georg BOLLWEG	Germany
Baiba BROKA	Latvia
Yusuf ÇALIŞKAN	Türkiye
Alfonso-Luís CALVO CARAVACA	Spain
Eugenia G. DACORONIA	Greece
Bénédicte FAUVARQUE-COSSON	France
Eesa Allie FREDERICKS	South Africa
Henry D. GABRIEL	United States of America
Arthur S. HARTKAMP	Netherlands
Hideki KANDA	Japan
Patrick KILGARRIFF	United Kingdom
In-Ho KIM	Republic of Korea
Alexander S. KOMAROV	Russian Federation
Antti T. LEINONEN	Finland
Ricardo L. LORENZETTI	Argentina
Niklaus D. MEIER	Switzerland
Attila MENYHÁRD	Hungary
José Antonio MORENO RODRÍGUEZ	Paraguay
Monika PAUKNEROVÁ	Czech Republic
Kathryn SABO	Canada
Jorge SÁNCHEZ CORDERO DÁVILA	Mexico
Luc SCHUERMANS	Belgium
Jingxia SHI	People's Republic of China
Carmen Tamara UNGUREANU	Romania