ELI
EUROPEAN
LAW
INSTITUTE

ELI Principles on the Use of Digital Assets as Security

Report of the European Law Institute

ELI

EUROPEAN
LAW
INSTITUTE

ELI Principles on the Use of Digital Assets as Security

Report of the European Law Institute

The European Law Institute

The European Law Institute (ELI) is an independent non-profit organisation established to initiate, conduct and facilitate research, make recommendations and provide practical guidance in the field of European legal development. Building on the wealth of diverse legal traditions, its mission is the quest for better law-making in Europe and the enhancement of European legal integration. By its endeavours, ELI seeks to contribute to the formation of a more vigorous European legal community, integrating the achievements of the various legal cultures, endorsing the value of comparative knowledge, and taking a genuinely pan-European perspective. As such, its work covers all branches of the law: substantive and procedural; private and public.

ELI is committed to the principles of comprehensiveness and collaborative working, thus striving to bridge the oft-perceived gap between the different legal cultures, between public and private law, as well as between scholarship and practice. To further that commitment it seeks to involve a diverse range of personalities, reflecting the richness of the legal traditions, legal disciplines and vocational frameworks found throughout Europe. ELI is also open to the use of different methodological approaches and to canvassing insights and perspectives from as wide an audience as possible of those who share its vision.

European Law Institute
Schottenring 16/175
1010 Vienna
Austria
Tel: + 43 1 4277 22101
E-mail: secretariat@europeanlawinstitute.eu
Website: www.europeanlawinstitute.eu

ISBN: 978-3-9505192-2-8

This publication was co-funded by the European Union's Justice Programme, the *Colegio de Registradores de España* (Spanish Land Registrars) and the International Union of Judicial Officers. Acknowledgment is also due to the University of Vienna which has generously hosted the ELI Secretariat under successive Framework Cooperation Agreements since 2011.

This project is co-funded by the European Union

universität wien

Registradores DE ESPAÑA

UIHJ

Table of Contents

Acknowledgements

Project Team
Project Reporters on Access to Digital Assets
Sjef van Erp (Professor (em), The Netherlands)
Jos Uitdehaag (Judicial Officer, The Netherlands)

Drafters of the ELI Principles on the Use of Digital Assets as Security
Phoebus Athanassiou (Legal Counsel and Associate Professor, Germany)
Teemu Juutilainen (Associate Professor, Finland)
Denis Philippe (Lawyer, Professor, Belgium)

Other Members of the Project Team
Gabriele Della Morte (Professor, Italy)
Wian Erlank (Professor, South Africa)
Sabine Heijning (Private International Law Consultant, The Netherlands)
Paul Matthews (Lawyer, Honorary Professor, UK)
Thomas Meyer (Law Reform Specialist, Germany)
Christopher Mondschein (Researcher, The Netherlands)
Christopher K Odinet (Professor, USA)
Radim Polčák (Professor, Czech Republic)
Albert Ruda (Professor, Spain)
Teresa Touriñán (Land Registrar, Spain)

Advisory Committee
Assessors
Reiner Schulze (Professor, Germany)
Christiane Wendehorst (Professor, Austria – until November 2021)
Aneta Wiewiórowska-Domagalska (Academic Counsellor, Germany)

Other Members
Suzanne Brown Walsh (Attorney-at-Law, USA)
Sergio Cámara Lapuente (Professor, Spain)
José Antonio Castillo Parrilla (Post-doctoral Researcher, Spain)
Richard Frimston (Consultant, UK)
José Llopis Benlloch (Notary, Spain)
Peter Lown, QC (Professor (em), Consultant, Canada)
Donna Molzan, QC (Barrister and Solicitor, Canada)

Members Consultative Committee
Jason Allen (Post-doctoral Fellow, UK)
Austrian Chamber of Civil Law Notaries (represented by Stephan Matyk-d'Anjony, Austria)
Arvind Babajee (Corporate Jurist & Chartered Management Accountant, Mauritius)
Curia of Hungary (represented by Mónika Gáspár, Hungary – until June 2021)
Moustapha Ebaid (Legal Researcher, Egypt)
European Law Students' Association Austria (represented by Anh Nguyen, Austria)
European Union of Judges in Commercial Matters (represented by Rainer Sedelmayer, France)
Karen Lynch Shally (Lecturer, Ireland)
Lineke Minkjan (Consultant, the Netherlands)
Dimitrios Moustakatos (Lawyer, Greece)
Cécile Sainte-Cluque (Notary, France)

School of Law, University of Hull (represented by Gonzalo Vilalta Puig, UK)
Society of Trust and Estate Practitioners (represented by Leigh Sagar, UK)
Ferenc Szilágyi (Lecturer, Hungary)
Aura Esther Vilalta Nicuesa (Senior Lecturer, Spain)
University of Latvia (represented by Vadims Mantrovs, Latvia)
Western University 'Vasile Goldis' Arad – Romania, Faculty of Law (represented by Christian Alunaru, Romania)

Observers
Spanish Land Registrars (represented by Silvino Navarro, Spain)
European Commission (represented by Maria Vilar Badia and Veronica Williams, Belgium)

ELI Project Officer
Katja Kolman (Senior Project Officer, Austria)

Executive Summary

The Principles address the use, by private parties, whether natural or legal persons, of digital assets as security for credit. In particular, the Principles are intended to focus on situations where the parties contractually agree to create a security interest in a digital asset, within the meaning of the Principles, so as to secure the performance by the security provider or another debtor of its secured obligation(s) vis-à-vis the secured creditor. The Principles treat the creation of a security interest in a digital asset as the creation, by contract, of a limited right in that asset, entitling the secured creditor to satisfaction of its claims vis-à-vis the security provider or another debtor. The right so created is to be construed as a right *in rem* or a functionally equivalent right, insofar as it entitles the secured creditor to enjoy priority over the security provider's other creditors. The Principles present definitions of key concepts in the use of digital assets as security, including one for 'digital asset', building on the core attributes of assets within the intended scope of the Principles. The creation of a security interest through a security agreement will typically be covered by a conflict rule built on some objective connecting factor. The Principles propose that the law applicable to the creation of security interests in digital assets be identified by reference to the place of business or central administration or habitual residence of the security provider. In those cases where a clear, readily identifiable connection exists between the digital asset under consideration and one particular jurisdiction, on account of the characteristics of that asset and the environment of its creation and holding, the Principles propose that the law governing the creation of a valid security interest in that digital asset should be the law of that jurisdiction, ie, the law of the digital asset itself. Additionally, the Principles address the issue of determining the applicable law in cases where the digital asset to be used as security represents a real-world asset, tangible or intangible. Regarding the third-party effectiveness of security interests, including their priority against competing claims, the Principles propose determining the applicable law similarly to that for the creation of a security interest in digital assets. For the purposes of both creation and third-party effectiveness, the Principles presuppose compliance with the requirements of the applicable law. However, where those requirements reflect the characteristics of more conventional assets and cannot be meaningfully applied to digital assets, the Principles cater for the necessary adaptations. Finally, under the Principles, a security interest is to be extinguished once there is full payment or other satisfaction of all secured obligations.

Project Reporters' Preface

The 'Access to Digital Assets' Project began as a feasibility study to determine whether the (revised) Fiduciary Access to Digital Assets Act, as promulgated by the (US) Uniform Law Commission (ULC) in 2015 (the 'ULC Model Law'), might serve as a workable model, also for Europe.[1] That, however, proved difficult. The ULC Model Law, which has proved to be a success, as it has been implemented in numerous US States, is limited to fiduciaries,[2] with the categories of fiduciaries that it covers consisting of personal representatives of decedents' estates, conservators for protected persons, agents acting pursuant to a power of attorney, and trustees. The purpose of the ULC Model Law is twofold: it is to give such fiduciaries, to the extent possible, powers of management concerning digital assets equal to such powers over physical assets and the power to deal with such assets, while at the same time respecting privacy and the intent of the user. The Access to Digital Assets Project Team took note of the fact that the concept of fiduciaries (and, especially, of trustees) is typical of the common law tradition, but it is less developed in the civil law tradition. Moreover, the Access to Digital Assets Project Team took note of the somewhat different final focus of the Access to Digital Assets Project, which looks at security rights, enforcement and possibly succession, matrimonial and registered partnership property. The Project Team also looked closely at a comparable model enacted by the Uniform Law Conference of Canada (the Uniform Access to Digital Assets by Fiduciaries Act of 2016) and considered the findings of comparative legal analysis and scholarly debate both in Europe and elsewhere in the world.[3] The success of both the American and the Canadian model laws made clear that there is an obvious practical need for guidance in this area. Therefore, it was decided that the feasibility study should result in a prospective project, which was eventually approved as a full ELI Project under Council Decision CD 2019/4.

The Access to Digital Assets Project, as finally approved, aims to clarify and facilitate the position of those claiming an entitlement to digital assets and all those who increasingly have to deal with digital assets in their daily legal practice, in particular, judges, lawyers, notaries public, public registrars and enforcement agents. The aim of the Project is to help bring coherence to, and promote the harmonisation of, existing laws and legal concepts relevant for access to digital assets. To achieve its aims, the Project proposes both substantive and conflict of laws principles. Substantive harmonisation, let alone unification, would be a complex and lengthy process, whereas solutions to practical legal problems arising in connection with the use of digital assets are needed now already. Accordingly, the Project does not seek to provide a model law-type solution, independent of the substantive law prescriptions of the existing legal systems. Instead, it seeks to provide guidance based on which national legal systems can address the challenges that the use of digital assets poses. As a general proposition, national legal systems are well equipped to address these challenges, provided that help is at hand with identifying *which substantive law rules apply to the relevant legal questions* and *what adaptations may be necessary to the existing rules* (insofar as the latter have been developed with conventional assets in mind). It is this type of guidance that the Project seeks to provide, through a combination of substantive and conflict of laws principles.

The structure of the full Project is quite broad. Originally, its goal extended to identifying the various categories of digital assets, the types of persons who may wish or need to have access to them, and the settings in which questions of access could arise, followed by a more category-specific approach with a focus on digital assets as security for credit, digital assets under succession, the matrimonial or registered partnership regime applicable to them, and enforcement against digital assets. As the work of the Project Team matured, it became apparent that, in the case of a financial institution requiring access to, for instance, crypto-assets where

[1] See <www.uniformlaws.org/committees/community-home?CommunityKey=f7237fc4-74c2-4728-81c6-b39a91ecdf22>.
[2] See <www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=112ab648-b257-97f2-48c2-61fe109a0b33&forceDialog=0>, p 1.
[3] See <www.ulcc.ca/images/stories/2016_pdf_en/2016ulcc0006.pdf>.

these are offered as security for a loan, a different approach was needed compared to the situation of an heir who seeks to gain access to crypto-assets or other digital objects of value that are part of a deceased's estate or a judicial enforcement officer wishing to enforce a judgment. As work on the Project progressed, developments accelerated, resulting in the decision not to present a full Project report but, rather, to present its results in instalments.

The first instalment, which is now published, was prepared by a specialised small working group consisting of Phoebus Athanassiou, Teemu Juutilainen and Denis Philippe, and subsequently shaped in discussions among the broader Project Team and the external participants, following ELI procedures. This instalment concerns access to digital assets in a financial setting.[4] The term 'access' does not yet have a clear and precise meaning, which is why the Project Team has refrained from presenting any legal definition thereof. The Principles proposed in this first instalment cover all of the main aspects of using a digital asset as security for credit and dealing with it. As mentioned earlier, questions regarding applicable law are also dealt with in the Principles, despite the considerable uncertainty surrounding them, given the need for at least some initial legal guidance in this respect.[5]

The original purposes of the Access to Digital Assets Project have not changed over time. The Principles presented in this Report are intended as a source of inspiration and guidance for the further development of case law and legislation in the field of digital assets by international organisations and national legislatures. The Principles may also be used by judicial enforcement officers, public authorities, (civil law) notaries and commercial arbitrators whenever they need to deal with questions of relevance to access to digital assets. The Project does not deal with underlying substantive questions of legal qualification, regarding whether digital assets can be 'possessed' or 'owned'. The present set of Principles, therefore, uses a generalised notion of security interest, the concrete meaning of which will depend on the relevant national law.

The Access to Digital Assets Project is closely related to the Principles for a Data Economy Project, undertaken jointly by the American Law Institute (ALI) and ELI, but the two serve different purposes. Whereas the ALI-ELI Project focused on data transactions and on data rights, with data understood as records of large quantities of information, the Access to Digital Assets Project focuses on a similar range of digital assets, but in selected, specific settings: security and judicial enforcement. It may consider, in the future, succession, matrimonial and registered partnership property. Originally, the ALI-ELI Project had included an already fully-drafted Chapter on security rights in data, which was later taken out of the ALI-ELI Project, inter alia to avoid inconsistencies between the two Projects, and was provided to the Project Team as a source of inspiration.

The Project has attracted considerable (worldwide) attention. In the course of the Project, the Project Reporters were in contact with the International Monetary Fund (IMF), the World Bank, the Society of Trust and Estate Practitioners (STEP) and the Council of Bars and Law Societies of Europe (CCBE). They also participated in work in this area by the United Nations Commission on International Trade Law (UNCITRAL), the International Institute for the Unification of Private Law (UNIDROIT) and the International Union of Judicial Enforcement Officers (UIHJ-IUJO). Other institutions have also shown great interest in the project.

The Project was financially supported by ELI, the European Union (EU), the International Union of Judicial Enforcement Officers and the Council of Land, Commerce and Movable Property Registrars of Spain.

[4] Future instalments will concern access to digital assets as part of judicial enforcement and may concern access to digital assets as part of a succession, or a matrimonial or registered partnership property regime.

[5] On related developments in the HCCH, see <https://assets.hcch.net/docs/f787749d-9512-4a9e-ad4a-cbc585bddd2e.pdf>.

List of Abbreviations

ALI	American Law Institute
BCBS	Basel Committee on Banking Supervision
CCBE	Council of Bars and Law Societies of Europe
DeFi	decentralised finance
DLT	distributed ledger technology
ELI	European Law Institute
ESMA	European Securities and Markets Authority
EU	European Union
FATF	Financial Action Task Force
FCD	Financial Collateral Directive
FMLC	Financial Markets Law Committee
G7	Group of Seven
HCCH	Hague Conference on Private International Law
IMF	International Monetary Fund
MiCA	Markets in Crypto-Assets (Proposal for a Regulation)
MiFID II	Markets in Financial Instruments Directive II
NFT	non-fungible token
PIL	private international law
PREMA	primary residence of the encryption private master keyholder
PROPA	place of the relevant operating authority/administrator
RUFADAA	Revised Uniform Fiduciary Access to Digital Assets Act
STEP	Society of Trust and Estate Practitioners
UCC	Uniform Commercial Code
UIHJ-IUJO	International Union of Judicial Enforcement Officers
UNCITRAL	United Nations Commission on International Trade Law
UNIDROIT	International Institute for the Unification of Private Law
ULC	Uniform Law Commission

ELI Principles on the Use of Digital Assets as Security – Black Letter Principles

1 Scope and Purpose

1. The Principles apply to the use of digital assets as security by private parties, whether natural or legal persons, in accordance with the terms of a security agreement, and are intended for use across legal systems, but primarily in the EU.

2. The Principles do not apply to non-consensual security interests, ie, security interests created by operation of law rather than by voluntary disposition (agreement).

3. The Principles do not apply to the seizure of digital assets by public bodies in the exercise of their public powers.

4. The Principles are without prejudice to the treatment of digital assets already regulated as financial instruments under national law and, where applicable, EU or other supranational law, and they are not intended to derogate from any such law. Accordingly, in the event of any inconsistency between the Principles and such other law, the latter prevails.

2 Digital Assets as Security

1. A digital asset can be used as security in accordance with the terms of a security agreement between a security provider and a secured creditor (the 'Parties').

2. The use of a digital asset as security is subject to compliance with the provisions of the law governing the creation of security interests, under Principle 3, and to the law governing the effectiveness of security interests against third parties, under Principle 4.

3 Creation of Security Interests in Digital Assets and Applicable Law

1. To create a security interest in a digital asset, the Parties to a security agreement must comply with the requirements of the applicable law for the creation of a security interest of the type intended by the Parties.

2. For the purposes of Principle 3(1), the 'applicable law' is the law of the jurisdiction in which the security provider has, at the time of the creation of the security interest, its place of business, or its central administration (if it has a place of business in more than one jurisdiction) or the law of the jurisdiction in which the security provider has its habitual residence (absent a place of business).

3. By derogation from Principle 3(2), in those cases where the digital asset itself is clearly connected with one particular jurisdiction, the law of that jurisdiction is deemed to be the 'applicable law'.

4. If the digital asset to be used as security represents a real-world asset, tangible or intangible, the question of whether and under which conditions a security interest created in the digital asset would also result in the creation of a security interest in the underlying real-world asset is to be determined by reference to the ordinary conflict of laws rules governing the proprietary aspects with respect to that real-world asset.

5. If the applicable law makes the creation of a security interest in assets conditional on their physical delivery to the secured creditor, then that condition is deemed to be fulfilled in the case of a security interest created in a digital asset where the security provider has put the secured creditor in a position where the latter can exercise control over the digital asset concerned, even if short of the actual physical delivery of the real-world asset to the secured creditor.

6. The creation of a valid security interest over a digital asset depends on the security provider's rights in it and, in particular, on the security provider's power to encumber it, but without prejudice to the rights of bona fide secured creditors or other third parties, which are a matter of effectiveness and priority of security interests against third parties under Principle 4, and whether the description of the encumbered digital asset in the security agreement reasonably allows its specification.

7. The creation of a valid security interest over a digital asset need not depend on whether the security provider enjoys intellectual property rights over the encumbered digital asset. The eventual protection of a digital asset by intellectual property law does not prevent the creation, by the security provider, of a valid security interest in that asset, provided that the conditions set out earlier in this Principle are complied with.

8. The Parties to a security agreement may make provision for fluctuations in the value of the encumbered digital asset. Such provisions do not adversely affect the validity of the security interest, except where national law or commercial practice would dictate that fluctuations resulting in the market value of the digital assets transferred by way of security exceeding that of the debt owed to the secured creditor would qualify as an unconscionable or otherwise prohibited form of over-collateralisation.

4 Effectiveness of Security Interests in Digital Assets Against Third Parties and Applicable Law

1. To be effective against third parties, and to enjoy priority over their interests, a security interest in a digital asset must fulfil, where applicable, the requirements for effectiveness against third parties concerning the type of security interest intended under the applicable law.

2. For the purposes of Principle 4(1), the 'applicable law' is the law of the jurisdiction in which the security provider has, at the time of the creation of the security interest, its place of business or its central administration (if it has a place of business in more than one jurisdiction) or the law of the jurisdiction in which the security provider has its habitual residence (absent a place of business).

3. By derogation from Principle 4(2), in those cases, where the digital asset itself is clearly connected with one particular jurisdiction, the law of that jurisdiction is deemed the 'applicable law'.

4. If the digital asset to be used as security represents a real-world asset, tangible or intangible, the question of whether and under which conditions third-party

effectiveness achieved with respect to a security interest in digital asset also results in third-party effectiveness of a security interest in the underlying real-world asset is to be determined by reference to the ordinary conflict of laws rules governing the proprietary aspects with respect to that real-world asset.

5. For jurisdictions where a statutory transaction filing or notice filing system for security interests in respect of intangible assets exists, the effectiveness against third parties of a security interest in a digital asset, and its priority against competing claimants, including other secured creditors, and creditors of the security provider, can be achieved through compliance with that system, subject to any necessary adaptations.

6. For jurisdictions where neither a statutory transaction filing or notice filing system for security interests in respect of intangible assets nor any other system establishing third-party effectiveness and priority exists, a security interest in a digital asset becomes effective against third parties once the secured creditor has gained effective control of the digital asset, that is a degree of control sufficient to prevent the security provider from independently disposing of the digital asset.

5 Enforcement and Extinction of Security Interests in Digital Assets

1. In the event of the debtor's default, the secured creditor may enforce on the digital asset used as security in accordance with the provisions of the security agreement, also without the involvement of judicial instances, where allowed in the relevant jurisdiction, and subject to Principle 5(4).

2. Whether or not the debtor's default is attributable to its insolvency, within the meaning of Principle 5(3), or to a failure to comply with its contractual obligations vis-à-vis the secured creditor, the latter must act in good faith and proceed in a commercially reasonable manner in exercising its enforcement rights under Principle 5(1).

3. For the purposes of Principle 5(1), the term 'default' includes the debtor's insolvency, as defined by the laws of the relevant jurisdiction.

4. Where the debtor's default is attributable to its insolvency, within the meaning of Principle 5(3), the secured creditor's rights in a digital asset used as security are to be enforced in accordance with the applicable insolvency and enforcement laws.

5. Nothing in this Principle is intended to determine whether, with regard to a digital asset used as security, a third party owes a duty to the security provider or the secured creditor.

6. Unless otherwise provided for in the security agreement, a security interest is extinguished once all secured obligations have been discharged.

ELI Principles on the Use of Digital Assets as Security, Definitions and Comments

Definitions

For the purposes of the Principles, the following definitions apply:

a. 'control' in respect of a digital asset means the legal power or factual capability of any natural or legal person to deal in and/or extinguish such assets, as the case may be;

b. 'digital asset' means any record or representation of value that fulfils the following criteria:

(i) it is exclusively stored, displayed and administered electronically, on or through a virtual platform or database, including where it is a record or representation of a real-world, tradeable asset, and whether or not the digital asset itself is held directly or through an account with an intermediary;

(ii) it is capable of being subject to a right of control, enjoyment or use, regardless of whether such rights are legally characterised as being of a proprietary, obligational or other nature; and

(iii) it is capable of being transferred from one party to another, including by way of voluntary disposition.

It is irrelevant, for the purposes of this definition, what the design and operational features of the relevant platform or database are, or whether the relevant digital asset's protection against undue replication, transmission and/or use is dependent on the use of cryptography, or whether the relevant digital asset represents a monetary claim on (and, correspondingly, a liability of) an identifiable party as issuer, custodian or controller thereof or whether the asset in question fulfils the functions of money or currency.

c. 'intermediary' means an issuer of a digital asset who provides services in connection with its management and/or holding, and any third-party custodian involved in the digital asset's management and/or holding;

d. 'Principles' means the concrete principles enunciated in this Report;

e. 'secured creditor' means a party to a security agreement whose claims against a debtor are secured by a security interest in one or more digital assets, created under the terms of a security agreement;

f. 'security agreement' means any contractual arrangement, regardless of its form, between a security provider and a secured creditor that creates or aims to create a security interest in one or more digital assets;

g. 'security interest' means the right that a security provider grants to the secured creditor over a digital asset, enabling the secured creditor to have recourse to that asset in the event of the debtor's default in the performance of its contractual obligations vis-à-vis the secured creditor;

h. 'security provider' means any natural or legal person that is a party to a security agreement, under the terms of which it has granted to a secured creditor a security interest in one or more digital assets.

Comment:

The contemporary understanding of 'digital assets' – whose concrete definition is central to the Principles – associates that concept with the relatively recent emergence of distributed data storage technologies and their various applications. A survey of the field testifies both to the considerable breadth of the concept of 'digital assets' and, no less significantly, to the objective difficulty of defining digital assets in a universally acceptable way, whether on account of the vast array of different types of digital assets or due to the constant evolution in this space.[6]

By way of example, an IMF publication has defined digital assets as 'digital representations of value, made possible by advances in cryptography and distributed ledger technology. They are denominated in their own units of account and can be transferred peer to peer without an intermediary.'[7] The focus of the IMF definition is on crypto-assets (including cryptocurrencies) – a mere subset of digital assets – whose defining feature is that the value they embody is secured by cryptographic authentication within their native platform or database. For its part, the Financial Action Task Force (FATF) has defined a 'virtual asset' as 'a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. Virtual assets do not include digital representations of *fiat* currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations'.[8] The FATF's definition differs from that proposed in the IMF publication, as it places the emphasis on non-financial asset-type digital assets, while at the same time excluding from its scope centrally-issued, digital equivalents of *fiat* money (which the IMF definition appears to capture). Interestingly, the Basel Committee on Banking Supervision (BCBS) has altogether refrained from proposing a definition, acknowledging that 'there is no single or generally-recognised definition of crypto-assets at present', and stressing that 'terms such as cryptocurrencies, virtual currencies, tokens, and coins are used in different contexts to refer to some or all types of crypto-assets'.[9] The Revised Uniform Fiduciary Access to Digital Assets Act (2015) (RUFADAA) – one of the reference points for the Principles – states that the term 'digital asset' means 'an electronic record in which an individual has a right or interest. The term does not include an underlying asset or liability unless the asset or liability is itself an electronic record.'[10] Last but not least, in its Markets in Crypto-Assets (MiCA) proposal, the European Commission has defined 'crypto-assets' to encompass any 'digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology'.[11]

The definition proposed in the Principles – whose scope of application covers crypto-assets and non-cryptographically authenticated digital assets alike, applying to them in the same manner – draws on the following *three* core attributes of digital assets: *first*, their *intangible nature*, which is reflected in their electronic-only storage, display and/or administration, even where a particular asset represents a tangible, real-world asset; *second*, the subsistence in them of a *right of control, enjoyment or use, lato sensu* – defined as the right to access and enjoy the non-traditional form of value that a digital asset embodies – which, in conjunction with their digital format, renders their transfer and subsequent use technically possible and commercially desirable;

---

[6] Some authors have proposed broad and inclusive definitions, treating most data stored in digital form as 'digital assets'. Others have resisted the inclusion of cryptocurrencies, considering them to be a distinct phenomenon. Yet others have reduced 'digital assets' to cryptocurrencies, treating the two as synonyms.

[7] Donge He, 'Monetary Policy in the Digital Age' IMF Finance & Development, June 2018, Vol 55, No 2 <www.imf.org/external/pubs/ft/fandd/2018/06/central-bank-monetary-policy-and-cryptocurrencies/he.pdf>. The rationale of this definition is similar to that of the definitions of 'distributed ledger technology' and 'crypto-assets' for the purposes of Article 3 (1)(1) and (2) of the Commission proposal for a Regulation of the European Parliament and the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM (2020) 593 final (MiCA) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0593&from=EN>.

[8] FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, Recommendations', October 2020 <www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>.

[9] BCBS, 'Designing a Prudential Treatment for Cryptoassets', December 2019 <www.bis.org/bcbs/publ/d490.htm>.

[10] The RUFADAA is available at <www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=112ab648-b257-97f2-48c2-61fe109a0b33&forceDialog=0>.

[11] Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM (2020) 593 final (MiCA) <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0593&from=EN>.

and *third*, their transferability (which may have to be determined by reference to the law governing their creation[12]). Implicit in the suitability of digital assets as security is their *value*, which is to be understood in economic terms, and which may attach to the asset itself (for instance, in the case of a cryptocurrency or a digital-only security) or to a privilege or service associated with it (for instance, in the case of a social networking user account, an online gaming account or a utility token) or to a tangible, or other real-world asset underlying a digital asset or guaranteeing its price stability (for instance, in the case of an asset-backed token or a stablecoin).

The Principles have no bearing on the legal characterisation of a digital asset and, in particular, on whether a given asset embodies a contractual, proprietary or other, *sui generis* right. Indeed, the novelty of digital assets makes it difficult to apply to them a classic property or contract law analysis. Although the question of their legal characterisation cannot be addressed *in abstracto*, ie without reference to their particular features, which vary across different types of digital assets, there is a growing consensus that, notwithstanding their electronic nature, digital assets can be the object of exclusive control, whether legal or factual, and that, therefore, security interests can be created in them. This is because, unlike some forms of data, digital assets can have the attribute of certainty, to the extent that they are *first* amenable to exclusive and substantial control and *second* assignable.

The types of assets falling within the proposed definition include s*ocial media and other online accounts* (but not the individual personal data stored in them) provided that *measurable value* attaches to them and no insuperable obstacle stands in the way of their assignment (such as, for instance, a contrary provision in a valid user agreement),[13] *cryptocurrencies*[14] and *stablecoins*,[15] uncertificated financial assets that only exist electronically, in the form of *tokens*, such as s*ecurity tokens*, including those held in accounts with intermediaries, *non-financial asset-type tokens* (including *utility*[16] and certain *payment*[17] tokens), and *hybrid tokens*.[18] What the above types of assets have in common is, on the one hand, their rivalrous nature[19] and, on the other hand, their novelty, on account of which they are not, as a rule, the object of comprehensive EU or national law regulation, whether with regard to the conditions for their use as security or more broadly. Moreover, it follows from the foregoing examples of digital assets that the proposed definition captures both 'pure' digital assets (ie digital assets that have been created and only exist in the digital world, in the form of tokens representing a unique set of valuable attributes, such as cryptocurrencies, security tokens, and social media accounts) and *asset-backed tokens* (ie digital representations of already existing,

[12] In the case of digital assets representing claims, that law is to be determined by reference to Article 14(2) of Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I).

[13] Social media and other online accounts can be of measurable value where they belong to celebrities or public figures with personal brand capital to which their online activities, through those accounts, may contribute, for instance, by disseminating their thoughts, ideas, and artistic or other, cultural output or by influencing the consumer choices of their 'followers' by endorsing specific products or services.

[14] The reference is to any virtual representation of value devoid of legal tender status that relies on the use of cryptography, rather than on a central issuing authority (such as a central bank, a credit institution or an e-money issuer), which can be transferred from one holder to another for the settlement of private debts. Examples include Bitcoin and Ether, respectively the first and second most popular cryptocurrencies to date, by market capitalisation.

[15] The reference is to a class of privately-issued cryptocurrencies that seek 'to stabilise [their] price ... by linking [their] value to that of a pool of assets', rendering 'stablecoins ... more capable of serving as a means of payment and store of value', and contributing 'to the development of global payment arrangements that are faster, cheaper and more inclusive than present arrangements' (see G7 Working Group on Stablecoins, 'Investigating the Impact of Global Stablecoins' October 2019, ii <www.bis.org/cpmi/publ/d187.pdf>). Facebook's *Diem* (formerly *Libra*) would be an example of a stablecoin.

[16] The reference is to a class of programmable digital asset that grants to its holder the right to exchange it in the future for products or services, actual or under development, digital or physical, that are provided (or are intended to be provided) by the token's issuer. Utility tokens both enhance their issuer's ability to quantify the value of the right that is the object of the token-issuance transaction and facilitate its transfer.

[17] The concept of payment (or currency) tokens refers to digital assets aimed to fulfil the properties of *fiat* money, although devoid of legal tender status. The reference, here, is to payment tokens that do not double as financial assets.

[18] Hybrid tokens are digital assets that share some of the characteristics of more than one digital asset classes (eg those of asset and utility tokens). A digital asset that both represents a share of ownership in a company and entitles its holder to the right to receive the first product or service that the said company manufactures would be an example of a hybrid token.

[19] The reference is to the economic quality of certain assets or goods that can only be used or consumed by a narrow number of people if their supply or value are not to be adversely affected. It is the risk of the depletion of their supply and the depreciation in their value that accounts for the intense competition ('rivalry') for their exclusive use and consumption.

physical assets, such as tokenised securities or bonds, tokenised gold-bullion, tokenised real estate or patents) and so-called 'non-fungible tokens' (NFTs), such as tokenised works of art or collectibles.[20]

Specifically in the case of social media and other online accounts (such as gaming accounts), the rationale of their inclusion in the scope of application of the Principles is as follows: although they are not records or representations of value in the same sense as other types of digital assets, and although their legal nature is, fundamentally, contractual, such accounts are capable of fulfilling all of the requirements of the definition of 'digital assets' proposed in the Principles. In particular, they exist (exclusively) in the digital world, they (may) embody value, they are subject to substantial (or, indeed, exclusive) control, and, depending on the terms of the contractual arrangement between the account holder and the account provider, and the judicial perception of the validity and enforceability of such arrangements, they may be transferable/assignable from one party to another. It is only in the case of online accounts fulfilling the above requirements that the Principles proposed here would apply.[21] It is, in any event, acknowledged, that the use as security of social media and online accounts can give rise to several complex legal questions,[22] which may render such use unattractive (but not legally impossible).

A few remarks are apposite on the concept of 'control' as used in this Report. The Principles opt for a hybrid concept of control over a digital asset, encompassing its legal 'possession' by a security provider (exemplified by the security provider's exercise of a legal right to control that digital asset, where the latter is recognised as an object of the law of property in a particular jurisdiction or otherwise enjoys a similarly protected legal status), but equally satisfied by the security provider's mere factual control over the digital asset tendered as security (exemplified by any form of control short of legal possession, including where a particular digital asset does not enjoy legal recognition, in a particular jurisdiction, as an object of the law of property). Legal or factual control will (or may) suffice for the creation of a security interest in a digital asset, but the only form of control relevant to the perfection of a security interest in a digital asset will be factual control. Apart from being the pertinent form of control for the perfection of security interests in digital assets, as well as that relevant for the application of Principles 3(5) and 4(6), factual control is also desirable to protect the interests of *bona fide* credit providers, who may lack the means through which to establish the security provider's title over a digital asset, but also, necessary for those digital assets in which proprietary rights, *stricto sensu*, may not subsist, given their particular features, which national laws may deem inconsistent with those of other, established objects of property law.

By way of illustration, the holder of a tokenised security, created under the laws of Member State X and recorded on a permissioned digital ledger will enjoy legal control over it (whether directly or through a custodian), provable by reference to the verifiable record that the digital ledger represents. In contrast, the holder of a cryptocurrency not enjoying recognition, in any relevant jurisdiction, as an object of property law that is recorded on a decentralised, non-permissioned ledger will merely enjoy factual control over it, which is co-terminous with the holder's (factual) control of the private key to the account where the cryptocurrencies tendered as security are held.

For the avoidance of doubt, the 'hybrid' concept of control advocated here does not import a requirement for 'control' over a digital asset to simultaneously display elements of both legal and factual control over that asset: either of the two will (or may) suffice for the creation of security interests in digital assets, with legal control often going hand in hand with factual control, while factual control will be

[20] NFTs are cryptographic, digital tokens, which represent objects in the real (or the digital) world, such as underlying works of art or collectibles, and may (but need not) embody ownership rights. Their creation and authentication rely mostly on the use of the Ethereum blockchain, utilising digital signatures to guarantee their uniqueness and indivisibility (hence, also, their non-fungibility). Though in existence for several years, they have only come to prominence closer to the time of publication of this Report, with demand for them having increased exponentially.

[21] It is submitted that the same would also apply to virtual tools or objects in existence within online gaming accounts (to the extent that these have economic value and may be transferrable from one player to another, also by way of security).

[22] These would include questions of relevance to the privity of contract between the social media and/or online account holder and the social media and/or online account provider, the account holder's personality (including privacy and identity rights), and any intellectual property rights of the account holder or the account provider.

the type of control necessary and/or sufficient for the perfection of security interests in digital assets and for the application of Principles 3(5) and 4(6).

Although digital assets will typically consist of digital 'data', grouped around a particular purpose and/or a particular person, the emphasis of the Principles is on the digital assets themselves, and on the question of their use as security, rather than on the underlying data, which, if *personal*, within the meaning of Article 4(1) of Regulation (EU) 2016/679 (GDPR), may not be the object of property rights, despite the fact that courts in some EU Member States have, in recent years, found that they may exhibit traits associated with the concept of property.[23]

The proposed definition of digital assets *is technology neutral*, not because their storage, display and administration are not technology-reliant but, rather, because the types of assets covered by this definition may be stored, displayed and administered on or through platforms or databases that are either centralised or decentralised, including platforms making use of blockchain-type technologies, defined as data validation technologies, where batches of validated transactions (or 'updates') are arranged in blocks linked sequentially to one another, through cryptographic tools, to preserve the full history of transactions over assets stored in them. Digital assets may, therefore, be stored on a blockchain, and be supported by a smart contract,[24] or, alternatively, on a non-blockchain database, including a publicly accessible cloud service or a restricted access 'data repository'.

The proposed definitions of 'intermediary', as well as those of 'secured creditor', 'security provider', 'security interest' and 'security agreement' are generic, drafted as they are in broad and functionalist terms, avoiding jurisdiction-specific terminology. Similar terminology is also used in several international instruments in the field of secured transactions, on which the Project Team drew for the purposes of its work.

[23] These questions were the object of reflection as part of the Principles for a Data Economy Project, undertaken jointly by ALI and ELI: < https://europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ALI-ELI_Principles_for_a_Data_Economy_Final_Council_Draft.pdf>. Regarding the question of property or other rights in co-generated data, the majority view was that no *fundamental* distinction should be made between personal and non-personal data. However, the fact that data is subject to data protection law represents a source of a restriction in terms of the ability of its use as security. On the link between that earlier project and the present one, the reader is referred to the Project Reporters' Preface, above. For a further analysis, see Ivan Stepanov, 'Introducing a Property Right over Data in the EU: The Data Producer's Right – an Evaluation' (2020) 34 (1) International Review of Law, Computers & Technology, 65–86.

[24] Smart contracts (defined as self-executing contracts written in coding language) may build on blockchain technology.

Principle 1:

1

Scope and Purpose

1. The Principles apply to the use of digital assets as security by private parties, whether natural or legal persons, in accordance with the terms of a security agreement, and are intended for use across legal systems, but primarily in the EU.

2. The Principles do not apply to non-consensual security interests, ie, security interests created by operation of law rather than by voluntary disposition (agreement).

3. The Principles do not apply to the seizure of digital assets by public bodies in the exercise of their public powers.

4. The Principles are without prejudice to the treatment of digital assets already regulated as financial instruments under national law and, where applicable, EU or other supranational law, and they are not intended to derogate from any such law. Accordingly, in the event of any inconsistency between the Principles and such other law, the latter prevails.

Comment:

Consistently with their purpose, whose focus is on the use by private parties (whether natural or legal persons) of digital assets as security for their transactions, in the course of the exercise of their economic freedoms,[25] the Principles do not cover the seizure of digital assets by public bodies in the exercise of their public powers, with a view to satisfying claims of the public authorities themselves, typically for the payment of taxes, duties, imposts or excises. The Principles are concerned with conventional credit, and may, but need not, cover credit provided by decentralised finance ('DeFi') platforms, which may (but need not) operate on the basis of smart contract protocols to automatically execute lending transactions (rather than directly between collateral providers and collateral takers) and which may offer services additional to secured lending, lying outside the scope of these Principles.

Besides, as the Principles do not seek to supplant but, rather, to complement and to build on existing legal prescriptions, in the event of any inconsistency between the Principles and the national or, where applicable, supranational laws to which the parties involved and/or any relevant contractual agreements or other types of legal relationship may be subject, such national or supranational laws will prevail.

The Principles are not intended to apply to situations where a security interest over digital assets may arise automatically by operation of law (for instance, by way of a statutory lien) and, hence, non-consensually (hence, outside the context of a private security agreement).

Finally, the Principles are without prejudice to digital assets already regulated as financial instruments under national law and, where applicable, EU or other supranational law, nor are they intended to derogate from any such law. Accordingly, the following types of assets, which already fall within the scope of dedicated EU legal or regulatory frameworks, are not covered by the Principles, despite fulfilling some of the core attributes of 'digital assets' listed above: 'financial

[25] Despite the Principles' focus on private parties, the Principles can also be applied to public parties (including publicly-owned private companies) when acting in a private capacity, that is, when engaging in regular, private law (contractual) relationships.

instruments', within the meaning of Article 4(1)(15) of the Second Markets in Financial Instruments Directive (MiFID II);[26] 'e-money', within the meaning of Article 2(2) of the Second E-Money Directive[27] (unless tokenised); 'deposits', within the meaning of Article 2(1)(3) of the Deposit Guarantee Schemes Directive;[28] 'structured deposits', within the meaning of Article 4(1)(43) of MiFID II; and any 'securitisation positions' (ie securities produced through a process of securitisation), in accordance with Article 2(19) of the Securitisation Regulation.[29] Moreover, the Principles do not apply to the creation of security interests over digital assets in the context of a financial collateral arrangement governed by the Financial Collateral Directive (FCD)[30] where the digital assets themselves qualify as 'financial instruments' within the meaning of Article 4(1)(15) of MiFID II,[31] or as claims relating to or rights in or in respect of financial instruments. For the benefit of the parties to financial transactions, and for the preservation of the soundness of the 'systems' in which they participate, within the meaning of the Settlement Finality Directive (SFD),[32] it is essential that the Principles do not interfere with the dedicated regime of the FCD and the SFD, which derogate from the (non-harmonised) national insolvency laws.[33]

[26] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU, OJ L173/349. It bears noting that draft Article 6(1) of the MiCA would amend the EU law definition of 'financial instrument' to expressly include within their scope '*(financial) instruments issued by means of distributed ledger technology*' (emphasis is ours).

[27] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC, OJ L267/7.

[28] Directive 2014/49/EU of the European Parliament and of the Council of 16 April 2014 on deposit guarantee schemes, OJ L173/149.

[29] Regulation (EU) 2017/2402 of the European Parliament and of the Council of 12 December 2017 laying down a general framework for securitisation and creating a specific framework for simple, transparent and standardised securitisation, and amending Directives 2009/65/EC, 2009/138/EC and 2011/61/EU and Regulations (EC) No 1060/2009 and (EU) No 648/2012, OJ L347/35.

[30] Directive 2002/47/EC of the European Parliament and of the Council of 6 June 2002 on financial collateral arrangements, OJ L168/43.

[31] In this regard, also see European Securities and Markets Authority, 'Advice on Initial Coin Offerings and Crypto-Assets' 9 January 2019, para 163, which was key to the Commission's approach in establishing the scope of application of the MiCA. The ESMA's recommendation, which the European Commission followed, was that where a crypto-asset qualifies as a 'financial instrument' within the meaning of MiFID II, it would remain subject to MiFID II as well as to any other EU rules applicable to MiFID II 'financial instruments', including the Prospectus Directive, the CSDR and the SFD.

[32] Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems, OJ L166/45.

[33] It is nevertheless acknowledged that the FCD may well apply to any underlying, real-world asset, which a digital asset, in the form of a token, may represent. Depending on the legal characterisation of the underlying, real-world asset as a financial instrument, the above overlap is inevitable, and it cannot be resolved by the Principles.

Principle 2:

2

Digital Assets as Security

1. A digital asset can be used as security in accordance with the terms of a security agreement between a security provider and a secured creditor (the 'Parties').

2. The use of a digital asset as security is subject to compliance with the provisions of the law governing the creation of security interests, under Principle 3, and to the law governing the effectiveness of security interests against third parties, under Principle 4.

Comment:

As mentioned earlier in this Report, the focus of the Principles is on the use, by private parties, of digital assets as security for their transactions, in the course of the exercise of their economic freedoms.

Principle 2(1) is declaratory in nature. Its aim is to draw the attention of the holders of digital assets to the possibility of using those assets as security, by relying on the Principles enunciated in this Report.

Digital assets will often embody considerable economic potential. The Principles propose practical ways through which private parties wishing to unlock that economic potential may do so, by using digital assets as security for credit. The possibility of using digital assets as security is unlikely to be present in the mind of, at least some, digital asset holders, on account of the relative novelty of digital assets, and the legal uncertainty surrounding their use as security for lending operations. One of the core objectives of the Principles is to create awareness of the possibility of using digital assets as security, so that some of their unused economic potential can be tapped into, if their holders wish to make use of that potential. For the avoidance of doubt, the Project Team takes no position on the advisability of the use of digital assets as collateral nor, indeed, on the suitability of certain types of digital assets, captured by the definitions proposed in these Principles, as security, given their individual characteristics and, in particular, their volatility, which, in some cases, will exceed that of more conventional assets, tangible or intangible.

Principle 2(2) seeks to introduce the substantive and conflict of laws principles enunciated later in the text. Accordingly, it states that use of a digital asset as security is subject to compliance with the provisions of the law governing the creation of security interests, as per Principle 3, and to the law governing the effectiveness of security interests against third parties, as per Principle 4. It bears noting that the law governing the asset itself may pose additional obstacles to use as security, which may also need to be considered in deciding on the feasibility (or otherwise) of such use. This would, for instance, be the case where a particular digital asset represents a claim.[34]

[34] It is recalled that, according to Article 14(2) of the Rome I Regulation, the law governing the assigned claim 'shall determine its assignability', while Article 14(3) states that the notion of assignment in Article 14 also includes 'transfers of claims by way of security and pledges or other security rights over claims'.

Principle 3:

3

Creation of Security Interests in Digital Assets and Applicable Law

1. To create a security interest in a digital asset, the Parties to a security agreement must comply with the requirements of the applicable law for the creation of a security interest of the type intended by the Parties.

2. For the purposes of Principle 3(1), the 'applicable law' is the law of the jurisdiction in which the security provider has, at the time of the creation of the security interest, its place of business, or its central administration (if it has a place of business in more than one jurisdiction) or the law of the jurisdiction in which the security provider has its habitual residence (absent a place of business).

3. By derogation from Principle 3(2), in those cases where the digital asset itself is clearly connected with one particular jurisdiction, the law of that jurisdiction is deemed to be the 'applicable law'.

4. If the digital asset to be used as security represents a real-world asset, tangible or intangible, the question of whether and under which conditions a security interest created in the digital asset would also result in the creation of a security interest in the underlying real-world asset is to be determined by reference to the ordinary conflict of laws rules governing the proprietary aspects with respect to that real-world asset.

5. If the applicable law makes the creation of a security interest in assets conditional on their physical delivery to the secured creditor, then that condition is deemed to be fulfilled in the case of a security interest created in a digital asset where the security provider has put the secured creditor in a position where the latter can exercise control over the digital asset concerned, even if short of the actual physical delivery of the real-world asset to the secured creditor.

6. The creation of a valid security interest over a digital asset depends on the security provider's rights in it and, in particular, on the security provider's power to encumber it, but without prejudice to the rights of bona fide secured creditors or other third parties, which are a matter of effectiveness and priority of security interests against third parties under Principle 4, and whether the description of the encumbered digital asset in the security agreement reasonably allows its specification.

7. The creation of a valid security interest over a digital asset need not depend on whether the security provider enjoys intellectual property rights over the encumbered digital asset. The eventual protection of a digital asset by intellectual property law does not prevent the creation, by the security provider, of a valid security interest in that asset, provided that the conditions set out earlier in this Principle are complied with.

8. The Parties to a security agreement may make provision for fluctuations in the value of the encumbered digital asset. Such provisions do not adversely affect the validity of the security interest, except where national law or commercial practice would dictate that fluctuations resulting in the market value of the digital assets transferred by way of security exceeding that of the debt owed to the secured creditor would qualify as an unconscionable or otherwise prohibited form of over-collateralisation.

Comment:

Both the creation of digital assets and the creation of security interests in them are areas of considerable fragmentation across different jurisdictions, with different legal systems drawing inspiration from rules applicable to more conventional asset classes.[35] Thus, different legal systems approach the question of the creation of security interests differently. Some jurisdictions distinguish between the requirements for creation and third-party effectiveness, while others apply the same set of requirements to both the creation of security interests and their third-party effectiveness (on third-party effectiveness, see Principle 4).

To determine the requirements for the creation of a security interest in an asset, one must first determine the law applicable to creation. The type of the asset in question and, in particular, its legal characterisation play a key role both in determining the applicable law but, also, in applying it, by helping to identify the types of security interest that can be created in an asset as well as the applicable requirements for creation (eg, in writing and/or by way of registration). The characterisation of a digital asset will depend on national law considerations: to take the example of cryptocurrencies, different jurisdictions have qualified these as 'currency', 'securities', 'investment contracts', 'commodities' or *sui generis* digital (intangible) assets.[36] Because questions of relevance to the creation of a security interest are jurisdiction-specific, the Principles strive to be jurisdiction-neutral. The premise of Principle 3(1) is compliance, to the extent possible, with the requirements of the applicable (national) law.

Regarding the determination of the applicable law, the starting point is that security agreements themselves are covered, in the case of EU Member State jurisdictions, by the Rome I Regulation (whose Article 3 allows the parties to choose the applicable law), but the creation of a security interest resulting from a security agreement is typically covered by a conflict rule built on some objective connecting factor, such as the *lex rei sitae* rule (as a result, the parties are generally not allowed to choose the law governing creation). The *lex rei sitae* rule is the general conflict rule for tangible assets and points to the location of the asset offered as security. Arguably, it may be possible to develop a *lex rei sitae* rule-type solution also for digital assets. This would require 'localising' digital assets in a particular jurisdiction by defining their 'location' for the purposes of the relevant solution. However, such an exercise could prove very difficult in the case of many digital assets, as digital assets typically have no physical location, with their notional 'location' often depending on various factors, including the manner of their holding. To take the example of Bitcoin, this may either be held directly on the Bitcoin ledger or through an online wallet (whether a custodian or a non-custodian wallet) or in a 'cold storage' device (typically, in the Bitcoin holder's personal computer or in another, 'remote' hardware storage device). Indeed, the various holding options could result in the same type of digital asset being 'localised' differently. Considering that other objective connecting factors may be available, it is not necessary and, presumably not advisable in many cases, to build conflict rules around the idea of the 'location' of the digital asset itself.[37]

To avoid the need for a case-by-case assessment of the circumstances of holding digital assets offered as security (which may change during the lifetime of a security agreement), Principle 3(2) proposes identifying the applicable law by reference to the place of business or central administration or habitual

---

[35] See Hague Conference on Private International Law (HCCH), 'Developments with Respect to PIL Implications of the Digital Economy, including DLT', Prel Doc No 4 of November 2020 <https://assets.hcch.net/docs/8bdc7071-c324-4660-96bc-86efba6214f2.pdf>. It may be uncertain whether digital assets can form part of a group of assets covered by an enterprise charge or other 'floating' (or 'all-assets') type of security interest. The mere fact that the legal norms on such security interests (in those jurisdictions where the creation of such interests is possible) may predate the emergence of digital assets should not prevent digital assets from being covered by 'floating' security interests.

[36] For a detailed account of the legal and regulatory treatment of cryptocurrencies in different jurisdictions see, *ex multi*, Phoebus Athanassiou, *Digital Innovation in Financial Services – Legal Challenges and Regulatory Policy Issues* (Kluwer Law International 2018), Ch 4; and HCCH, 'Report on the PIL Implications of the Digital Economy, including DLT' (November 2020), § 27 and accompanying footnotes.

[37] The challenges inherent in working through the PIL issues relevant to digital assets were acknowledged by the HCCH, in the following terms: 'PIL issues remain unresolved for situations involving such assets, agreements and operations. For example, there is clarity neither in relation to the applicable law to digital assets and corresponding transfers, nor in relation to the possibility of incorporating party autonomy and choice of law in DLT protocols. It is also not clear which State has the jurisdiction to resolve any corresponding disputes that may arise, with the very rare exception in which the dispute concerns transactions in which all nodes are located in one State (i.e., one-jurisdiction, permissioned systems). In addition, there is the issue of applicability and enforceability of choice of court agreements involving digital assets' (see HCCH (n 36), § 14).

residence of the security provider. The Principle draws on the general conflict of laws rule on security rights in intangible assets in the UNCITRAL Model Law on Secured Transactions (Articles 86 and 90), on the Report from the European Commission to the European Parliament, the Council and the European Economic and Social Committee on the question of the effectiveness of an assignment or subrogation of a claim against third parties and the priority of the assigned or subrogated claim over the right of another person,[38] as well as on the European Commission Proposal for a Regulation of the European Parliament and of the Council on the law applicable to the third-party effects of assignments of claims.[39] The rule proposed in Principle 3(2) has a number of advantages over potential alternatives: *first*, it is straightforward in its application, relatively stable and transparent vis-à-vis security takers; *second*, in situations where several creditors compete for the same digital asset as security, the rule proposed in Principle 3(2) has the advantage of providing a point of reference for deciding on the relative priority of competing claims; *third*, it is commonplace for the law of the place of the security provider to also govern insolvency proceedings, with the coincidence between the law of the security agreement and the relevant insolvency law thus appearing advantageous; *fourth*, the proposed rule would be beneficial in the context of simultaneous ('bulk') assignments of digital assets by the same security provider (these could, absent the rule proposed in Principle 3(2), be governed by different laws).[40] The members of the Project Team are aware that support for the default conflict of laws rule proposed in Principle 3(2) is not unanimous.[41] That said, the Project Team is of the opinion that, for the reasons set out above, and taking into account the specificities of digital assets, the solution proposed here is both legitimate and, overall, more advantageous, in terms of its practical application, compared to competing solutions.

In those cases where a readily identifiable connection exists between the digital asset under consideration and one particular jurisdiction, on account of the characteristics of that asset and the environment of its creation and holding, Principle 3(3) proposes that the law governing the creation of security interests in that digital asset should be the law of that jurisdiction, ie the law of the digital asset itself. Identifying that law would, at least in some cases, be relatively straightforward, and several examples are conceivable of what such a 'readily identifiable connection' might be. For instance, in the case of a permissioned distributed ledger technology (DLT) system, established by an identifiable issuer (or issuers) in an identifiable jurisdiction, operating subject to the laws of that jurisdiction and intended, *ab initio*, to operate within a single legal system, to the knowledge of all its permissioned participants, it would make sense if the creation of security interests in digital assets native to that system were to be subject to the law applicable to the system itself rather than to the law of the security provider. Examples of digital assets fulfilling these conditions include stablecoins, virtual currencies, NFTs and utility tokens, insofar as these are hosted in permissioned ledgers, operated by identifiable operators. The above example is to be contrasted to that of an 'intermediated' digital asset, defined as any digital asset that is held through a custodian or another intermediary, where the law of such custodian or intermediary could also be relevant in deciding on the system of law that is the

[38] Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the question of the effectiveness of an assignment or subrogation of a claim against third parties and the priority of the assigned or subrogated claim over the right of another person COM/2016/0626 final.

[39] Proposal for a Regulation of the European Parliament and of the Council on the law applicable to the third-party effects of assignments of claims COM/2018/096 final - 2018/044 (COD).

[40] For certain types of digital asset, namely those in permissionless, fully decentralised DLT systems, it may be difficult to conceive of other connecting factors if party autonomy is excluded. This point is implicitly made also by the FMLC (see FMLC, 'Distributed Ledger Technology and Governing Law: Issues of Legal Uncertainty' March 2018 <http://fmlc.org/wp-content/uploads/2018/05/dlt_paper.pdf>, para 7.6, 22).

[41] Reference is made, notably, to the work of the HCCH, which, despite having acknowledged the merits of the place of business or central administration or habitual residence of the security provider as a connecting factor, has also drawn attention to its potential limitations (see HCCH (n 36), Annex I, 10). Importantly, the HCCH has expressed no preference in favour of any of the 12 possible connecting factors listed in Annex I of its Report, which include, inter alia, the primary residence of the encryption private master keyholder (PREMA), (place of the relevant operating authority/administrator) PROPA and the law of the elective *situs*.

most closely connected with a security arrangement involving the use, as security, of such intermediated digital asset.[42,43] In its reflections on the private international law (PIL) challenges posed by digital assets native to a DLT system, the Financial Markets Law Committee (FMLC) has also discussed the idea of an 'elective *situs*' as a means of determining the system of law governing the proprietary aspects of digital assets native to a DLT system,[44] an approach that strikes the Project Team as legitimate.

Principle 3(4) addresses the specific case of digital assets that represent real-world assets, whether tangible or intangible. The question of whether, and under which conditions, a security interest created in the digital asset would also result in the creation of a security interest in the underlying real-world asset is to be decided by reference to the substantive law to which the ordinary conflict of laws rules governing the proprietary aspects regarding the underlying real-world asset would point (for example, the l*ex rei sitae* rule or the *lex registrationis* rule). By way of example, if the holder of a token created in a ledger operating in Country Y and representing a real-world asset (eg real estate) constituted under the laws of Country Y were to tender it as security to a creditor located in Country Z, then it is the laws of Country Y (ie the real estate's lex rei sitae) that would determine whether the security interest created in the token would also result in the creation of a security interest in the underlying real estate. This solution strikes a balance between legal certainty, on the one hand, and facilitating the use of assets created by new technologies, on the other hand, and it is also mindful of the dichotomy that the literature makes between the law of the token and the law of the main (underlying) asset as regards the conflicts of laws treatment of so-called 'exogenous tokens'.[45]

As a concession to the *sui generis* character of digital assets, and taking into account their intangible nature, Principle 3(5) proposes interpreting loosely the requirement enshrined in some national legal systems for the physical delivery of an asset as a precondition for the creation of a security interest in it.[46] Thus, the Principle is satisfied with any method through which the Parties can ensure that the secured creditor is in effective (direct or indirect) control of the digital asset offered and accepted as security, consistently with the secured creditor's security interest in it. Importantly, for the purposes of Principle 3(5), the secured creditor's control may be either direct or indirect (eg where an escrow agent is used). Examples of the latter include situations where a third-party escrow agent is involved in security-taking as a trusted holder of the digital assets intended for use as security.

Digital assets can be the object of intellectual property rights, including copyright, trademarks and patents. In some cases, the security provider's rights with respect to digital assets will be limited by a licensing agreement (or equivalent), granting other persons access to them, in exchange for valuable

---

[42] This is the approach tentatively opted for by UNIDROIT in the case of so-called 'non-native' digital assets (ie digital assets created and existing also outside the digital world). According to UNIDROIT, '[N]on-native digital assets require an interface, such as an intermediary organisation creating the digital token. From this point on, the PIL analysis depends on how the rights to non-native digital assets are understood (a claim against the intermediary?). The private international law question would follow that route, e.g., if that right were to be regarded as claim against the intermediary, the chosen law would apply or, in absence of that, the law determined by the relevant fallback rules. The most relevant scenario to be considered in this context involves the outflow of the underlying asset from the estate of the intermediary, and its subsequent insolvency. A conflict may emerge under these circumstances, between the acquirer of the underlying asset with the acquirer of the digital asset, potentially governed by two different laws …' (see UNIDROIT, Digital Assets and Private Law Working Group, Issues Paper, June 2021, 55–56).

[43] For a more thorough discussion of the various connecting factors see, in particular, Christiane Wendehorst, 'Digitalgüter im Internationalen Privatrecht' (2020) 40 (6) IPRax, 490–499 (Wendehorst 2020); and Matthias Lehmann, 'National Blockchain Laws as a Threat to Capital Markets Integration' (2021) Uniform Law Review, 1–32 <https://academic.oup.com/ulr/advance-article/doi/10.1093/ulr/unab004/6314582>.

[44] See FMLC, 'Distributed Ledger Technology and Governing Law: Issues of Legal Uncertainty' March 2018 <http://fmlc.org/wp-content/uploads/2018/05/dlt_paper.pdf>, according to which, '[P]articipants in the DLT system would be able, on this approach, contractually to choose the law governing ownership, transfer and use of assets', so that 'the proprietary effects of all transactions on the system would be subject to the same governing law' (ibid, paras 6.5–6.6, 15). Although the solution proposed by the FMLC involves a fair degree of party autonomy, it is not tantamount to allowing the parties to a security agreement to choose the law applicable to third-party relations, which would be inconsistent with some of the basic tenets of property law.

[45] See, in particular, Wendehorst 2020 (n 43), 496–497.

[46] Different jurisdictions may treat the same asset as a digital or a conventional asset. For instance, this may be the case with a token that represents an underlying, real-world asset: a given jurisdiction may treat the token as a digital asset, whereas another jurisdiction may look at the underlying, real-world asset instead, only treating the token as its digital representation, but not as an autonomous (digital) asset in its own right. Therefore, situations may exist where physical delivery is still relevant for an asset that is defined as a digital asset in the Principles, but which the national legislator in a given jurisdiction does not treat as a digital asset, still requiring its physical delivery as a condition for the creation of a security interest in it.

consideration. The licensor's residual rights in digital assets come with value, which renders them eligible as security, under the terms of a security agreement, irrespective of whether the digital assets in question (also) enjoy intellectual property law protection, which may limit the extent of the licensee's rights over them (for instance, by restricting the licensee's ability to grant a sub-licence). Under Principle 3(7), if the security provider has an interest in certain digital assets, the latter can be the subject matter of a security agreement, irrespective of whether intellectual property rights subsist in those digital assets. Put otherwise, security providers do not need to enjoy intellectual property rights in a digital asset before they can create a security interest in it (unless the use of the digital asset as security is provided for in a licensing requirement, as in the case of NFTs, whose holders acquire, by the act of investing in them, a non-commercial, own-use only *licence* to the intellectual property rights in the work that the NFT references).

The valuation of assets offered as security presents challenges, especially where these assets are intangible, as in the case of digital assets. Because of their intangible nature, and their characteristics, which may be conducive to a higher degree of volatility than in the case of more 'conventional' assets, digital assets used as security may appreciate or depreciate substantially in value during the lifetime of the security agreement. Where the Parties to a security agreement have chosen to make provision for fluctuations in the value of the digital asset, Principle 3(8) states that such a provision will not adversely affect the validity of their security agreement. Security agreements will typically specify the asset or property being held as collateral under the agreement, including its description by type, quantity and, crucially, value. The inclusion, in a security agreement, of a mechanism for the valuation of the digital asset or assets tendered and accepted as collateral, to cater for potential fluctuations in value, should not vitiate the legal effect and the enforceability of that agreement by rendering it ambiguous, vague or indefinite. Principle 3(8) is without prejudice to any contrary provisions or doctrine under the law of contract governing the security agreement.

Principle 4:

4

Effectiveness of Security Interests in Digital Assets Against Third Parties and Applicable Law

1. To be effective against third parties, and to enjoy priority over their interests, a security interest in a digital asset must fulfil, where applicable, the requirements for effectiveness against third parties concerning the type of security interest intended under the applicable law.

2. For the purposes of Principle 4(1), the 'applicable law' is the law of the jurisdiction in which the security provider has, at the time of the creation of the security interest, its place of business or its central administration (if it has a place of business in more than one jurisdiction) or the law of the jurisdiction in which the security provider has its habitual residence (absent a place of business).

3. By derogation from Principle 4(2), in those cases where the digital asset itself is clearly connected with one particular jurisdiction, the law of that jurisdiction is deemed the 'applicable law'.

4. If the digital asset to be used as security represents a real-world asset, tangible or intangible, the question of whether and under which conditions third-party effectiveness achieved with respect to a security interest in a digital asset also results in third-party effectiveness of a security interest in the underlying real-world asset is to be determined by reference to the ordinary conflict of laws rules governing the proprietary aspects with respect to that real-world asset.

5. For jurisdictions where a statutory transaction filing or notice filing system for security interests in respect of intangible assets exists, the effectiveness against third parties of a security interest in a digital asset, and its priority against competing claimants, including other secured creditors, and creditors of the security provider, can be achieved through compliance with that system, subject to any necessary adaptations.

6. For jurisdictions where neither a statutory transaction filing or notice filing system for security interests in respect of intangible assets nor any other system establishing third-party effectiveness and priority exists, a security interest in a digital asset becomes effective against third parties once the secured creditor has gained effective control of the digital asset, that is a degree of control sufficient to prevent the security provider from independently disposing of the digital asset.

Comment:

Comparative studies show that the requirements for the effectiveness of security interests against third parties vary greatly from one jurisdiction to another, even in Europe.[47] Often, these requirements relate to the need for publicity of security interests. While most legal systems require security arrangements to be made public, both the types of security interest subject to those requirements and the means of fulfilling them vary between jurisdictions. Typical means include dispossessing the security provider of the encumbered asset, notifying a certain person of the existence of the security interest, and registration.

[47] See, generally, Eva-Maria Kieninger (ed), Security Rights in Movable Property in European Private Law (Cambridge University Press 2004).

Registration systems come in different models. They may be indexed by assets or by persons, and they may involve transaction filing or notice filing, which differ from each other in the extent and specificity of the data recorded in the relevant register.[48] In some jurisdictions, both the creation of security interests and their third-party effectiveness are subject to the fulfilment of the same requirements, while in others, third-party effectiveness may be conditional on the fulfilment of certain additional steps – sometimes referred to as 'perfection', following the terminology of Article 9 of the Uniform Commercial Code (UCC).[49]

Principle 4 assumes, by default, compliance with the requirements for third-party effectiveness under the 'applicable law'. The applicable law is determined similarly to that for the creation of a security interest in digital assets under Principle 3. For reasons of clarity and practicability, it is submitted that the same conflict of laws rules should be used for both purposes, and there appear to be no weighty reasons for differentiation.[50]

Compliance with the requirements for third-party effectiveness under the applicable law is required 'where applicable' (Principle 4(1)) and 'subject to any necessary adaptations' (Principle 4(5)). Where those requirements have been designed with more conventional assets in mind and cannot be meaningfully applied to digital assets, the parties may adapt the requirements in their security agreement to make those requirements fit the characteristics of the digital asset in question. The understanding underlying the Principle is that the adapted requirements are to perform functions similar to those of the requirements applicable to more conventional assets.

For example, if the original function of a requirement applicable in a given jurisdiction is to transfer actual physical possession of the assets provided as security (including to the custody of a trustee) so as to prevent the security provider from disposing of the digital assets during the lifetime of the security interest (ie, before repayment of the secured debt), then a suitable adaptation could consist in the use, by the Parties, of alternative means of control, affording the secured creditor a measure of control over the digital asset materially equivalent to that of the surrender of physical control over tangible assets. These considerations underlie the text of Principle 4(6).

Principle 4(4) shares the same philosophy and is motivated by the same public policy and practicability considerations as those underlying Principle 3(4), above. Thus, in common with Principle 3(4), Principle 4(4) points to the ordinary conflict of laws rules governing the proprietary aspects of the real-world asset referenced by a token as decisive on the question of whether, and subject to which conditions, third-party effectiveness achieved with respect to a security interest in the token would also result in third-party effectiveness of a security interest in the underlying real-world asset. An illustration is apposite. If a debtor in Country X has pledged tokens representing real-world, tangible assets, in respect of which the relevant conflict rule is *lex rei sitae*, and if the underlying tangible assets are located in Country Y, then it is the law of Y that would determine whether, and under which conditions, third-party effectiveness of the pledge of the tokens would also result in third-party effectiveness of a pledge of the tangible assets.

[47] See, generally, Eva-Maria Kieninger (ed), Security Rights in Movable Property in European Private Law (Cambridge University Press 2004).
[48] See Sjef van Erp, 'The Cape Town Convention: A Model for a European System of Security Interests Registration?' (2004) 12 European Review of Private Law, 91.
[49] It is recalled that the perfection methods set out in Article 9 of the UCC consist of filing (statutory notice registration), possession and control.
[50] In this regard, also see UNCITRAL, 'Legislative Guide on Secured Transactions' 2010, X. Conflict of Laws, para 18; and UNCITRAL, 'Model Law on Secured Transactions' 2016, Articles 85–86.

Principle 5:

5

Enforcement and Extinction of Security Interests in Digital Assets

1. In the event of the debtor's default, the secured creditor may enforce upon the digital asset used as security in accordance with the provisions of the security agreement, also without the involvement of courts, where allowed in the relevant jurisdiction, and subject to Principle 5(4).
2. Whether or not the debtor's default is attributable to its insolvency, within the meaning of Principle 5(3), or to a failure to comply with its contractual obligations vis-à-vis the secured creditor, the latter must act in good faith and proceed in a commercially reasonable manner in exercising its enforcement rights under Principle 5(1).
3. For the purposes of Principle 5(1), the term 'default' includes the debtor's insolvency, as defined by the laws of the relevant jurisdiction.
4. Where the debtor's default is attributable to its insolvency, within the meaning of Principle 5(3), the secured creditor's rights in a digital asset used as security are to be enforced in accordance with the applicable insolvency and enforcement laws.
5. Nothing in this Principle is intended to determine whether, with regard to a digital asset used as security, a third party owes a duty to the security provider or the secured creditor.
6. Unless otherwise provided for in the security agreement, a security interest is extinguished once all secured obligations have been discharged.

Comment:

In catering for the enforcement of security interests over digital assets, the Principle seeks to promote flexibility and efficiency of the enforcement process. Accordingly, Principle 5(1) provides for extra-judicial enforcement, though subject to any restrictions laid down in the applicable insolvency law, for example, for the orderly carrying out of insolvency proceedings. At the same time, Principle 5(2) renders the extra-judicial exercise of a secured creditor's post-default rights subject to an overarching obligation to exercise those rights in good faith and in a commercially reasonable manner. Although the Principle does not expressly provide for recourse to a court or other judicial body to resolve disputes arising in relation to the extra-judicial exercise of a secured creditor's post-default rights, it is understood that either party may seek relief in case the other party fails to comply with its contractual or other related obligations.

Under Principle 5(4), where the debtor's default is attributable to its insolvency, the secured creditor's rights in a digital asset used as security are to be enforced in accordance with the applicable insolvency and enforcement laws. Digital assets are intangibles and, as a result, they cannot be seized and enforced upon as one would hope to do with tangibles. The modalities for the enforcement of a secured creditor's rights in them will depend on their nature. For instance, if the digital assets used as security are tokens, which have been given as (non-possessory) security to a secured creditor, the latter would need to have access to the debtor's private key to gain access to and realise the pledged tokens. There is, naturally, a real risk that the insolvent debtor may refuse to grant access to the private key. One way to circumvent this risk is for the security agreement to foresee the debtor's entry, with a third party, into an escrow agreement, and the

transfer to that third party of the private key to the tokens. Acting as escrow agent, the third party would cooperate with the secured creditor, in the event of the debtor's insolvency, for the enforcement of the creditor's security right, eg for an enforced sale of the tokens to satisfy the secured creditor's claim.[51]

Considering the contractual nature of the relationship between the Parties to a security agreement, Principle 5(5) carves out from its scope the duties that third parties may be subject to, vis-a-vis the Parties, with regard to the digital assets used as security (for example, the duties of confidentiality that social network platforms owe to the holders of social network accounts).

Finally, in accordance with standard practice in all of the jurisdictions represented in the Project Team, Principle 5(6) states that a security interest is extinguished once there is full payment or other satisfaction of all secured obligations. This would apply to situations where a debtor who has defaulted on the secured obligations agrees to pay the lender the full amount owed together with any expenses incurred in taking, holding and preparing for the disposition of the digital asset used as security, including, if so stated in the security agreement, any legal expenses incurred by the secured creditor.

[51] Other alternatives are conceivable. One example is recourse to a smart contract between a lender and a borrower, written on a blockchain or other, DLT-run platform (including that of a wallet provider). The aim of the smart contract would be to automate the process of the realisation of collateral in the event of the borrower's default on her repayment obligation or, alternatively, that of its release, in the event of the borrower's compliance with her repayment obligation.

Sources and Final Notes

The types of security interest in movable assets (tangible or intangible), the requirements for their creation and the conditions for their effectiveness against third parties (including the security provider's other creditors, secured or unsecured) vary greatly across European jurisdictions. The same is true of the legal characterisation of movable assets.

At the time of writing, the EU does not have a common framework for secured transactions comparable to what the UCC provides in the United States.[52] Book IX (Proprietary security in movable assets) of the Draft Common Frame of Reference does not provide such a framework and it appears unlikely to do so in the foreseeable future – whether *de jure* or *de facto*.

Considering the divergences of secured transactions laws in the EU, these Principles have been drafted in broad and functionalist terms, avoiding, to the extent possible, jurisdiction-specific terminology. Moreover, to ensure the ability of the parties to private security arrangements to invoke them, and in order to facilitate the use of digital assets as security for credit, the Principles have been drafted with the intention that they should, to the extent possible, operate in tandem with any applicable national secured transactions laws, avoiding, to the extent possible, the question of the exact legal characterisation of rights in digital assets as rights *in rem* or rights *in personam*.

The Project Team has drawn on the following main sources of inspiration to draft the Principles: (a) Book IX (Proprietary security in movable assets) of the Draft Common Frame of Reference; (b) Chapters I-III and VII of the UNCITRAL Model Law on Secured Transactions; (c) the Uniform Law Commission's Fiduciary Access to Digital Assets Act (Revised, (2015)); (d) the UCC; (e) the RUFADAA; (f) the work of the FMLC on the intersection between DLTs and PIL (March 2018); (g) the work of the HCCH on the PIL implications of the digital economy, including DLT (November 2020); (h) the subject matter relevant work of the UNIDROIT (June 2021); and (i) the European Commission's Proposal for a Regulation of the European Parliament and of the Council on the law applicable to the third-party effects of assignments of claims.[53]

---

[52] See Kristin Johnson, Sarah E Hsu Wilbur and Stanley Sater, '(Im)Perfect Regulation: Virtual Currency and Other Digital Assets as Collateral' (2018) 21 Science and Technology Review, 115, suggesting that the focus of the US discussion is on whether digital assets fit into the asset categories of Article 9 – or other provisions – of the UCC, and on the problem of perfection.

[53] See <www.consilium.europa.eu/en/press/press-releases/2021/06/07/assignments-of-claims-council-approves-mandate-for-negotiations/>.

The European Law Institute (ELI) is an independent non-profit organisation established to initiate, conduct and facilitate research, make recommendations and provide practical guidance in the field of European legal development. Building on the wealth of diverse legal traditions, its mission is the quest for better law-making in Europe and the enhancement of European legal integration. By its endeavours, ELI seeks to contribute to the formation of a more vigorous European legal community, integrating the achievements of the various legal cultures, endorsing the value of comparative knowledge, and taking a genuinely pan-European perspective. As such, its work covers all branches of the law: substantive and procedural; private and public.

ELI

EUROPEAN
LAW
INSTITUTE

ISBN: 978-3-9505192-2-8