Guide on legal issues relating to the use of distributed ledger technology in trade

United Nations
Commission on International Trade Law

Further information may be obtained from:

UNCITRAL secretariat, Vienna International Centre
P.O. Box 500, 1400 Vienna, Austria

Telephone: (+43-1) 26060-4060
Internet: uncitral.un.org Email: uncitral@un.org

UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAW

Guide on legal issues relating to the use of distributed ledger technology in trade

UNITED NATIONS
Vienna, 2025

Note

Symbols of United Nations documents are composed of capital letters combined with figures. Mention of such a symbol indicates a reference to a United Nations document.

UNITED NATIONS PUBLICATION
Sales No.: E.26.V.2
ISBN 978-92-1-157732-7
e-ISBN 978-92-1-154683-5

The designations employed and the presentation of material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities or concerning the delimitation of its frontiers or boundaries.

Information on uniform resource locators and links to Internet sites contained in the present publication are provided for the convenience of the reader and are correct at the time of issue. The United Nations takes no responsibility for the continued accuracy of that information or for the content of any external website.

This publication has not been formally edited.

Publishing production: Publishing Section, United Nations Office at Vienna.

Preface

At its fifty-fifth session, in 2022, the United Nations Commission on International Trade Law (UNCITRAL, or "the Commission") authorized the publication of the Taxonomy of legal issues related to the digital economy[1] (the Taxonomy) (A/77/17, para. 165), which developed out of exploratory work carried out by the secretariat to identify topics for possible future work by UNCITRAL to address the applications of emerging digital technologies in trade. Building on Part five of the *Taxonomy*, on distributed ledger systems, at the same session UNCITRAL requested the secretariat to prepare a guidance document on legal issues relating to the use of distributed ledger systems in trade (A/77/17, paras. 22(f) and 169).

At its fifty-sixth session, in 2023, the Commission had before it a note by the secretariat on the scope of the work to be conducted (the "scoping paper") (A/CN.9/1146). The Commission noted with appreciation the content of the scoping paper and highlighted its intersection with other digital trade workstreams of UNCITRAL such as the work carried out by Working Groups II, IV and V. Broad support was expressed for the work to be carried out in close coordination with other concerned international organizations, and its relevance for several projects undertaken by the Hague Conference on Private International Law (HCCH) was noted (A/78/17, paras. 200–202). Accordingly, the Commission requested the secretariat to continue its work on the preparation of a guidance document on legal issues relating to the use of distributed ledger systems in trade, within existing resources and in cooperation with other concerned organizations, as appropriate (A/78/17, para. 22(e)).

At its fifty-seventh session, in 2024, the Commission had before it a note by the secretariat on legal issues relating to the use of distributed ledger technology in trade (A/CN.9/1175). It was indicated that the note usefully established a link between distributed ledger technology and UNCITRAL texts and that the glossary was particularly valuable (A/79/17, para. 288). Broad support was expressed for the secretariat to continue its work, including in cooperation with other organizations. After discussion, the Commission requested the secretariat to continue and finalize its work (A/79/17, paras. 289–290).

At its fifty-eighth session, in 2025, the Commission had before it a draft guidance document on legal issues relating to the use of distributed ledger technology in trade (A/CN.9/1222). Broad appreciation was expressed for the guidance document. After discussion, the Commission authorized publication in electronic form of the guidance document, incorporating the descriptive elements of decentralized autonomous organizations set out in a document on legal issues relating to the use of decentralized

[1] *UNCITRAL Taxonomy of legal issues related to the digital economy*, United Nations publication, Sales No. E.12.V.11.

autonomous organizations in trade (A/CN.9/1225), in all official languages of the United Nations (A/80/17, para. 161). Consistent with that authorization, the UNCITRAL secretariat prepared for publication this guide on legal issues relating to the use of distributed ledger technology in trade.

Contents

Introduction

1. The present guide provides guidance on legal issues relating to the use of distributed ledger technology in trade. It is intended to offer commercial operators a list of legal matters that they may wish to consider when contemplating the use of distributed ledger technology (DLT). Furthermore, it may be useful for non-commercial operators, including intergovernmental organizations, and also aims to support the implementation of Recommendation 6 of the Report of the Joint Inspection Unit, Blockchain applications in the United Nations system: towards a state of readiness (JIU/REP/2020/7). In keeping with the principle of technology neutrality that underpins UNCITRAL texts, it does not provide advice on whether DLT is the appropriate technology for the intended use.

2. The guide consists of three parts and a glossary. Part one provides basic background on DLT, offering a short technical overview, followed by a brief discussion of the types of distributed ledgers and by an illustration of their main features. This background aims to familiarize the reader with technical notions that have legal relevance.

3. Part two discusses legal issues relating to the use of distributed ledger technology in trade by addressing three fundamental questions. The first question is which legal issues are relevant for selecting the appropriate DLT system. The second question is which rights and remedies are available in the case of malfunctioning of the DLT system. The third question is which legal issues should be considered when using DLT to provide commercial services.

4. Part three illustrates how UNCITRAL texts and principles may apply to the use of DLT, with focus on the delivery of commercial services. A glossary of technical terms completes this guide.

5. This guide contains use cases and case studies. The first occurrence of each defined technical term contained in the glossary is in italics.

6. The Permanent Bureau of the HCCH has provided inputs and comments on private international law issues discussed in this guide in the framework of the ongoing coordination and cooperation activities between UNCITRAL and HCCH.

Part one.

Background

A. What is distributed ledger technology?

7. The notion of DLT encompasses a broad array of technological systems that enable the decentralized recording, sharing and synchronization of data across multiple participants. Among the various forms of DLT, blockchain has emerged as the most prominent and widely recognized implementation. At its core, DLT is a technology for data storage that may be used generally for recording information contained in data messages, or for specific applications that leverage the technical features of DLT. The use of DLT in general, and of blockchain in particular, has often been associated with *smart contracts*, tokens (including *non-fungible tokens* (NFTs), semi-fungible tokens, and *soulbound tokens*) and cryptocurrencies.

8. The Taxonomy (para. 172) offers a working definition of DLT:

> "in terms of a bundle of technologies and methods that are deployed to implement and maintain a ledger (or database) that is shared, replicated and synchronized on multiple networked computers (or servers). Thus, a distributed ledger technology system ("DLT system") is the system (comprising software and hardware components) that supports the deployment of those technologies and methods. DLT systems differ in their design, governance, purpose and use".

9. Initially introduced for peer-to-peer transfers of value,[1] the use of blockchain evolved from a single-purpose transactional ledger to a general-purpose digital public infrastructure for diverse use cases.

10. DLT systems, especially those which are private and custom-built, are designed with a specific focus in mind and do not operate beyond their boundaries. They are comprised of several components such as a decentralized information technology infrastructure, an Internet connection and data. DLT systems are based on cryptography and generally include dedicated technology such as a *cryptographic hash*

[1] Satoshi Nakamoto, "A Peer-to-Peer Electronic Cash System", 2008. Unlike prior attempts, this suggestion was implemented at scale with bitcoin.

function (for instance, of the data in a block), a *consensus mechanism* (for example, *proof of stake*), and digital assets (for example, tokens).

B. How does distributed ledger technology work?

11. Blockchain is a form of DLT that utilizes a chain of blocks to store data. Each block comprises data, such as a transaction log, and a summary – often a cryptographic hash – forming a link to the preceding block. Various models of DLT systems are available, in particular with regard to giving access to data and ability to modify the ledger. These models can be further tailored to specific needs and preferences. Commercial operators should assess carefully the features of the DLT system they consider using in light of their business needs.

12. Key characteristics of all distributed ledgers include:

- **Integrity:** the use of cryptographic techniques ensures the integrity of the network by relying on trust in the system instead of trust in a single central controlling entity. This approach is called "trustless" as it does not require any external source of trust. However, multiple mechanisms to build trust, such as organizational tokens in decentralized autonomous organizations (DAOs) (see paras. 54–56 below), are used in DLT systems; and
- **Pseudonymity:** users and participants in the ledger are often identified with pseudonyms.

13. Distributed ledgers are traditionally classified based on two key features: public or private ledger, and permissioned or permissionless participation in the network. This classification may assist in understanding the features of each type of distributed ledger.

14. The public or private nature of distributed ledgers refers to who can contribute to maintaining the DLT system as a *node operator*, that is the operator of a computer that is part of the system. The term "public ledger" denotes a decentralized system that permits unhindered access to the information stored on the ledger. Conversely, in a private ledger access is restricted to a selected group of pre-identified participants.

15. The permissioned or permissionless nature of distributed ledgers refers to whether permission is required prior to participating in the ledger, that is whether identification of the user is a precondition to participation. In a permissionless distributed ledger, no identification is required; in theory, any user may participate in the distributed ledger without identification. In a permissioned distributed ledger, users are required to identify themselves before being granted access to the distributed ledger, and measures for identity management are usually in place.

16. Hence, a public permissionless distributed ledger is the most open and decentralized model of distributed ledger. In this case, anyone may access, view, and record in the ledger without identity verification, prior permission or authorization by an administrator. Because of its open nature, this type of distributed ledger is scalable. Many widely used cryptocurrency protocols are based on public permissionless ledgers.

17. Key characteristics of public permissionless distributed ledgers include:

- **Open access:** no single administrator controls the network, thus effectively limiting the influence of any single actor on the network;
- **Open source:** the source code is publicly available, and anyone can propose modifications to it; and
- **Transparency:** all data on the distributed ledger is publicly visible although *pseudonymity* and other mechanisms may allow some privacy.

18. In contrast, a private permissioned ledger restricts the number of users of the ledger and requires users' identification prior to accessing, viewing and recording in the ledger. This type of ledger is often created, operated, used and controlled by the same commercial operator.

19. Key characteristics of private permissioned distributed ledgers include:

- **Restricted access:** only actors authorized by administrators can access and participate in the ledger;
- **Closed source:** code in the form deployed for the ledger is often not publicly available;
- **Controlled environment:** only selected actors may access the ledger;
- **Privacy:** data may be protected for privacy and confidentiality purposes due to restricted access to the ledger; and
- **Faster transaction speed:** due to the simplified *consensus mechanism*, a higher number of transactions may be performed in the same unit of time.

20. Public permissionless ledgers and private permissioned ledgers are at the respective ends of the range of DLT systems. It is possible to have hybrid models, that is a public permissioned ledger or a private permissionless ledger. A public permissioned ledger requires participants to identify themselves before they can participate in the ledger, although there is no restriction on who can participate in the ledger. A private permissionless ledger sets restrictions on participation but does not require participants to identify themselves. Commercial services tend to favour these hybrid models.

Use case: Examples of public permissioned ledgers

The European Blockchain Services Infrastructure (EBSI), developed under the European Digital Innovation and Cooperation (EDIC) framework, is an example of a public permissioned ledger. EBSI supports various use cases, including digital identity, notarization and education credentials. Users need to apply to EDIC to access EBSI.

In Latin America, Lacchain, a public permissioned DLT infrastructure spearheaded by the Inter-American Development Bank, promotes digital inclusion by enabling blockchain applications for financial inclusion, public records and supply chain management.

Similarly, the Blockchain-based Service Network (BSN) in China operates as a public permissioned ledger that facilitates access to blockchain technology for businesses and public institutions. BSN's permissioned nature allows for regulatory oversight while maintaining the benefits of a public, accessible infrastructure.

C. What are the distinctive features of distributed ledger technology?

1. Persistence of information

21. The procedure for modification of data recorded in a block entails modification of subsequent blocks, which cannot realistically be carried out in sufficiently developed distributed ledgers. Consequently, unilateral modifications of data are unlikely, and data recorded on the blockchain is relatively persistent. *Persistence of information* (or "immutability") is thus a defining feature of DLT, especially blockchain.

22. This feature may be recognized in the law, for instance by attributing a presumption of integrity and accuracy of the chronological ordering of the data stored on DLT. Under the European Union (EU) eIDAS Regulation, as revised,[2] the use of a trust service named "qualified electronic ledger" is associated with a presumption of the unique and accurate sequential chronological ordering and the integrity of data records contained therein when certain additional conditions are met. In article 3, point 52 of the same Regulation, "electronic ledger" is defined as "a sequence of

[2] Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC ("eIDAS Regulation"), OJ L 257, 28.8.2014, pp. 73–114, ELI: http://data.europa.eu/eli/reg/2014/910/oj, as amended by Regulation (EU) No. 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No. 910/2014 as regards establishing the European Digital Identity Framework, OJ L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj.

electronic data records, ensuring the integrity of those records and the accuracy of the chronological ordering of those records".

23. Assurance of information persistence may have significant legal consequences when rights need to be recorded to be effective. For example, in those security rights registries where prior registration of a security right may give priority (see UNCITRAL Legislative Guide on Secured Transactions,[3] rec. 76, subpara. (a)), the timestamping function associated with DLT may provide reliable assurance of the time of the registration. Moreover, if all assets of an enterprise are recorded correctly on DLT, it may be easier to identify their existence (though not necessarily assess their value). This may be useful, for instance, for facilitating access to credit and for consideration of pre-insolvency restructuring.

2. Interoperability

24. Modern digital trade is based on data flows ideally covering the whole range of commercial operations (a notion known as "end-to-end trade digitalization") to fully enable data analysis and reuse. The achievement of this goal is based on technical interoperability among different applications, which, in turn, is favoured by technology neutrality and the adoption of common standards. The absence of the principle of technology neutrality in the law may hinder "legal interoperability" and mutual legal recognition, and eventually, technical interoperability. Likewise, the lack of technical interoperability may practically affect "legal interoperability" and mutual legal recognition.

25. Distributed ledgers are generally not designed to interact with another distributed ledger or with non-DLT applications. This may further hinder interoperability and dataflows as information remains in a *data silo* and cannot be easily transmitted to or used in other systems.

26. Therefore, the development of common technical standards for distributed ledgers may improve interoperability, allowing information and assets to move seamlessly across DLT systems. Work has started to overcome technical limitations[4] and to define common technical standards.[5] Additional legal work to facilitate dataflows has also begun, including at UNCITRAL Working Group IV on default rules for data provisions contracts.

[3] *UNCITRAL Legislative Guide on Secured Transactions*, United Nations publication, Sales No. E.17.V.1.

[4] See, for example, the Cross-chain by Chainlink protocol, and the Polkadot Network ecosystem.

[5] See, for example, the work programme of the ISO/TC307 technical committee on blockchain and DLT.

27. The availability of technical and legal standards may reduce the risk of data silos in DLT systems and enable dataflows among applications. Examples of such business applications pertain to linking discrete electronic transferable records, such as bills of lading and bills of exchange, relating to the same business transaction and issued on different platforms, that are compliant with the UNCITRAL Model Law on Electronic Transferable Records (MLETR).[6]

[6] *UNCITRAL Model Law on Electronic Transferable Records* (2017), United Nations publication, Sales No. E.17.V.5.

Part two.

Legal Issues Relating to the Use of Distributed Ledger Technology in Trade

28. Understanding the legal framework applicable to DLT systems and to DLT-based services is essential to addressing the challenges posed by DLT. Determining the appropriate legal framework often involves considering three key pillars: (1) laws governing DLT systems and the provision of DLT, including contract law, property law and liability principles that underpin the legal rights and obligations of DLT participants, and related private international law rules; (2) electronic transaction laws, data privacy and protection regulations and data management frameworks; and (3) specific provisions tailored to DLT features, such as the treatment of smart contracts, *pseudonymity, persistence of information* and decentralization. Together, these pillars provide a structured approach to navigating the intersection of DLT and legal obligations, promoting both innovation and accountability.

29. Different approaches are possible to describe legal issues related to the use of DLT. The Taxonomy refers to two layers, the infrastructure layer and the application layer, and acknowledges that more layers may be identified for illustrative purposes (Taxonomy, para. 174). This guide focuses on the perspective of the commercial operator who intends to use DLT for interaction with clients or for internal business purposes.

A. What legal issues are relevant when considering a distributed ledger technology system?

30. DLT offerings vary widely, ranging from proprietary solutions tailored by private entities to open source frameworks deployed across decentralized networks. Commercial operators wishing to use DLT in their business face the fundamental choice of developing in-house DLT systems or outsourcing them to a third-party developer. Such choice depends on the scale of their operations, among other considerations.

Case study: Environmental considerations

Some regulators are increasingly concerned about the environmental footprint for distributed ledger *mining*. In particular, the *proof of work consensus mechanism*, which forms the basis of DLT for cryptocurrencies such as bitcoin, requires high energy consumption to verify that transactions have been executed on the distributed ledger.[a] Reducing energy usage caused by the *proof of work* mechanism is desirable and several initiatives aim to decarbonize the cryptocurrency industry.[b] From a technical standpoint, the move from the *proof of work* to the *proof of stake consensus mechanism* may reduce energy consumption in relation to *mining*.[c] Commercial operators that engage in *mining* or more generally use DLT should be aware of relevant regulations, including those establishing financial obligations related to the carbon footprint of DLT.

[a] On the environmental impact of distributed ledger mining, see Chamanara, S. & Madani, K. (2023). *The Hidden Environmental Cost of Cryptocurrency: How Bitcoin Mining Impacts Climate, Water and Land*, United Nations University Institute for Water, Environment and Health (UNU-INWEH), (Hamilton, Ontario, Canada, 2023).

[b] For example, the Crypto Climate Accord is an initiative on the decarbonization of distributed ledger mining.

[c] The Ethereum network moved from the *proof of work* mechanism to the *proof of stake* mechanism, which significantly decreased energy usage and carbon footprint.

1. Counterparty vetting

31. Counterparty vetting is critical to ensuring the reliability and security of DLT-based operations, particularly in a global trade environment. However, doing so requires the availability of technical and regulatory standards to be used as benchmarks. By complying with these standards, DLT providers not only improve the quality and transparency of their offerings but also strengthen user protection measures and reduce risks.

32. Counterparty risks can be significantly reduced if commercial operators conduct due diligence on DLT providers, for example, by ensuring that they are contracting with a legally recognized entity and verifying the company's track record of building and maintaining DLTs. In such cases, especially when using permissioned distributed ledgers, the counterparty risk may be similar to contracting with a regular service provider in any given industry. Moreover, when regulatory frameworks are available,[7] compliance of DLT services with those frameworks may give commercial operators additional confidence in their use.

[7] For example, Cyberspace Administration of China, Blockchain Information Management Regulations, January 2019.

33. Risks may further decrease when using private permissioned distributed ledgers because of the clear identification of the developer counterparty. Moreover, there is generally clarity on the terms under which the code of such distributed ledgers has been developed and deployed. (For additional considerations on counterparty vetting DAOs, see paras. 48–49 below.)

2. Business continuity management and assurance of service standards

34. *Business continuity management* (BCM) is the process of ensuring that an organization can continue to operate despite a disaster, disruption or other exceptional event. This includes identifying potential threats and vulnerabilities, developing and implementing plans to mitigate or prevent those threats and testing and maintaining those plans to ensure that they are effective. *Service level management* is the process of defining, agreeing and measuring the performance and quality of services that an organization provides to its customers. This includes setting service level targets, monitoring service level delivery and taking corrective action when necessary to ensure that service levels are being met. Business continuity and adequate *service level management* are crucial in building confidence in the use of distributed ledgers. The adoption of DLT would typically require amending existing BCM plans to tailor them to the features of DLT.

35. When procuring a DLT system on the market, commercial operators should verify that the DLT service provider has adequate BCM plans and identify which minimum level of service should be met. Due diligence, coupled with a contract that clearly sets out the rights and obligations of the parties, can reduce the chances of non-performance by the DLT service provider. Due diligence may take place during counterparty vetting but also during service provision. Possible measures include requesting the operational track record of the developer, requesting the balance sheets or profit and loss statements to assess the developer's financial condition and basic online research about the developer's reputation and prominence. In addition, commercial operators may establish in-house guidelines or policies on minimum standards that third-party service providers must meet before contracting with them.

36. Alternatively, if a commercial operator directly operates the DLT system and offers it for use or access to third parties, it becomes responsible for maintaining a certain level of service as developer, DLT service provider or both. Those commercial operators may set out their own BCM plans and indicate the expected minimum standard of service.

3. Audit procedures and the right to audit

37. Confidence in the deployed DLT system may be bolstered through third-party independent audits of the distributed ledger's code, of the developer and of the operator. Audit procedures include undertaking a *distributed ledger audit* to detect dysfunctional or fraudulent codes and identify any potential vulnerabilities or weaknesses in the DLT system.

38. Commercial operators may consider inserting in their contracts with developers and DLT providers a clause that grants them the right to audit the code, including any third-party developer's code. As this code could be implemented in the commercial operator's own information systems, the right to audit and an agreement on the modalities of the audit are important mechanisms to protect commercial operators against risks, including cybersecurity attacks exploiting errors in the code.

4. Contractual terms

39. The terms of use and associated policies of the DLT service provider play a critical role in defining rights and obligations of service providers and their clients. Commercial operators should consider incorporating specific terms into contracts with DLT providers, such as clauses that address liability, intellectual property rights and conflict resolution mechanisms, whenever contractual terms may be individually negotiated.

40. Harmonized policies on contractual clauses may contribute to creating a consistent standard of user protection, fostering trust and accountability across diverse market participants. By adopting such policies and transposing them in contractual terms, DLT providers can mitigate risks while ensuring equitable treatment and transparent interactions among parties.

Case study: Terms of use of a service provider

Providers active in trade digitalization often use DLT to deliver electronic trade documents. Those providers may utilize a third-party distributed ledger to offer services to financial institutions, who in turn incorporate those services into their offerings to clients. Electronic trade documents providers therefore operate as an interface between the distributed ledgers and the commercial entity offering financial services. The following clauses may be found in the terms of use of electronic trade documents providers:

- **User liability:** users are expected to utilize the service provider platform appropriately, ensuring the confidentiality of access information such as system passwords and user identities. They must also safeguard documents and cryptographic keys when storing and managing documents;

- **Prohibited activities:** actions that could compromise the platform's integrity, including unauthorized access attempts, introducing malicious code and overloading the system, are prohibited;
- **Disclaimer of liability:** the service provider disclaims liability for the accuracy of the documents supplied through its application and for any delays, errors or interruptions in service. It is also not responsible for the integrity of documents if software other than its proprietary software is used for storage of documents and cryptographic keys;
- **Risk disclosure:** users are informed about potential risks, such as unauthorized third-party access and the possibility of computer viruses, emphasizing the importance of taking precautions;
- **Amendments to terms:** the service provider reserves the right to amend and update the terms of use at any time with the latest version posted on its website. The service provider may also update, change or withdraw the business solution without obtaining prior user consent.

Commercial operators using such services should read carefully the terms of use, in particular with regard to expected diligence in handling electronic documents and the information system, including signature creation devices. They should also ensure the accuracy of the information entered in the system, especially given its persistence when stored on distributed ledgers.

B. How is a distributed ledger technology system managed?

41. DLT systems may malfunction for different reasons, including software bugs, vulnerabilities, etc. In traditional computing, the client of a service provider has recourse on a contractual and, possibly, other basis. However, the peculiar structure of distributed ledgers and the possible absence of a central administrator may hinder any legal action.

42. Governance of distributed ledgers operates on two distinct aspects, each addressing crucial aspects of system operation and service delivery. The first aspect pertains to how data is stored across the nodes of the DLT network and the ledger is maintained with a *consensus mechanism* (also called consensus protocol). Often described as the "brain logic" of the system, consensus mechanisms coordinate data transfers, ensuring that all nodes agree on the validity and sequence of transactions. This is fundamental to maintaining the integrity, security and decentralization of the ledger.

43. The second aspect pertains to how services are delivered on the DLT system, which often incorporates governance tools such as dedicated tokens and DAOs. Governance tokens allocate decision-making rights, enabling stakeholders to vote on key issues such as protocol upgrades and resource allocation. DAOs, on the other hand, offer a decentralized structure for managing decisions. Together, these aspects provide a framework for both the technical operation and the administrative oversight of DLT systems.

1. Basic features of DAOs

44. The increasing use of DLT systems has led to the creation of a specific type of computer code known as DAO to govern them. At its core, a DAO is a specific type of computer code used to manage distributed ledgers. A DAO possesses a governance structure, based on DLT, that relies on the use of token-based voting and smart contracts for decision-making, and lacks centralized management.

45. As an organizational entity, the DAO gathers participants with similar goals and may be used to offer commercial and non-commercial services. Being an organization, DAOs often operate globally, necessitating cross-border recognition of governance and liability frameworks.

46. DAOs can be used for commercial or other purposes besides their original DLT governance function and have been implemented across various industries. DAOs are also being considered as a new model to foster digital collaboration in line with cooperative values. In industries that rely on collaborative, multiparty networks for manufacturing, supply chain management and other operational functions, DAO-based cooperatives could potentially enhance transparency, reduce operational costs and increase member engagement, aligning with the goals of fostering digital innovation and inclusivity.

Governance structure of DAOs

47. Typically, DAOs operate through self-imposed rules or codes of conduct that reflect the operational framework, decision-making processes and objectives of the DAO. However, these rules do not carry the same binding legal force as governance documents for corporations, such as by-laws, articles of incorporation or corporate policy statements. While the traditional corporate model balances inclusivity and accountability, providing checks through defined roles and regulatory oversight, in most cases DAO governance rules are expressed in a way that resembles guidelines or community standards, rather than legally binding contracts or regulatory compliance statements.

48. Commercial operators that use or otherwise interact with a DAO should clearly understand the risks associated with these decentralized organizations. Mitigating measures include verifying the legal status of the DAO and requiring the DAO to identify its members and developers. The importance of predeployment testing, ongoing monitoring and contingency frameworks to safeguard the DAO's operations and member assets should be noted.

49. Commercial operators should conduct thorough due diligence on the DAO's governance structure, operational mechanisms and technical framework. This includes assessing the robustness of the DAO's governance structure, evaluating the mechanisms for decision-making and dispute resolution, and understanding the distribution of voting power and financial resources among its members.

50. The following technical features of a DAO may pose challenges that commercial operators need to consider when interacting with a DAO or otherwise using DAOs in their business:

- The rules for decision-making and *consensus* in a DAO are typically encoded in algorithms with the intention of fostering decentralized and transparent governance. However, these rules may become rigid as the DAO grows in size, complexity and scope of operations because amending automated rules logic often requires agreement among several stakeholders;
- Consensus mechanisms that function efficiently in smaller groups may struggle with scalability, resulting in prolonged deliberation times or gridlock in larger DAOs;
- The decision-making process in a DAO is typically distributed among its members which, while promoting inclusivity, can dilute individual responsibility. This may lead to mismanagement of the DAO's resources;
- Representation in a DAO's governance structure is often determined by holding specific digital assets or tokens. Such a representation mechanism risks concentrating power in the hands of a small group of wealthy participants and token holders while those with fewer tokens or lower financial investment in the DAO may feel excluded. Over time, these grievances can escalate into conflicts or disengagement, weakening the DAO's cohesion and effectiveness;
- DAOs rely heavily on DLT and automated software execution (referred to as smart contracts) to take and enforce governance decisions, making them dependent on the security and integrity of the underlying code. When vulnerabilities or errors are discovered, the difficulty of amending software code, often requiring community consensus and technical expertise, can leave DAOs exposed for extended periods to cyberthreats or operational inefficiencies.

51. The contractual framework may offer a first venue for clarifying rights and obligations of DAO participants. The governance documents for DAOs are often accessible to the public as white papers on websites or decentralized applications. Nevertheless, the non-binding nature of these documents, which are often written in non-legal language, can limit their legal effect.

52. In the absence of centralized management, the *consensus mechanism*, for example, by majority vote or by algorithms, and the dispute resolution mechanism are of great importance. Automated transactions are instrumental in self-executing operational decisions. By embedding governance rules in smart contracts, DAOs can automate actions such as proposal submissions, voting procedures and fund allocations or market transactions based on voting outcomes.

53. The UNCITRAL Model Law on Automated Contracting with Guide to Enactment (MLAC)[8] deals with legal aspects of contract automation on a technology neutral basis. Therefore, the MLAC applies to DLT-based smart contracts incorporating a contractual will, that is expressing a statement relevant for contractual purposes. Contractual parties who wish to have legal certainty on the use of automated contracts, including in the context of DAOs, may choose as applicable law, the law of a jurisdiction that has enacted the MLAC or incorporate the provisions of the MLAC as contractual terms.

Case study: The DAO hack

Because of the use of a *consensus mechanism*, and depending on the governance and type of DLT, vulnerabilities may be exploited to modify information on the ledger and affect *persistence of information*. For instance, in a *proof of work* distributed ledger, a group of validators controlling more than 50 per cent of the network's mining hash rate can alter the digital ledger. However, in practice, once a distributed ledger reaches a certain size, the requirement to control more than 50 per cent of the network's hash rate for unilateral modification of information is less likely to materialize due to its high cost.[a] This means that, the larger the distributed ledgers, the less vulnerable is the information stored therein.

In certain cases, especially as a response to a malicious attack, the governing entity of the distributed ledger may decide to make a change (known as a hard fork) to the *consensus mechanism* that is not compatible with existing blocks in the blockchain. Such a decision may affect *persistence of information* on the ledger, thus impacting DLT users as data stored therein may not be reliable.

[8] *UNCITRAL Model Law on Automated Contracting with Guide to Enactment*, United Nations publication, Sales No. E.25.V.4.

The hack of The DAO in 2016 involved the exploitation of a vulnerability in the code of "The DAO", an Ethereum-based DAO designed for community-driven investment. An attacker manipulated a software bug in The DAO's *smart contract*, siphoning approximately 3.6 million Ether (ETH), worth around $50 million at the time, into a separate child DAO controlled by the hacker. The incident led to a controversial hard fork of the Ethereum blockchain, splitting it into Ethereum (ETH) and Ethereum Classic (ETC), to reverse the hack and return the stolen funds to the original investors.

[a] This is the price to be paid for purchasing at market rate, the cryptocurrency needed to be in control of 51 per cent of the distributed ledger.

Use of tokens for governance of DAOs

54. DAOs may restrict decision-making participation to members who hold governance tokens. These tokens serve two purposes: they represent a financial stake in the DAO and grant voting rights. In practice, the weight of a member's vote is often proportional to the amount of governance tokens they hold. This model incentivizes financial or operational contributions to the DAO, as tokens are typically acquired through initial investment, contribution to the DAO (e.g. software development or content creation) or other forms of support like marketing.

55. In many cases, DAOs reward early contributors, also known as backers, with governance tokens to promote long-term participation and loyalty. However, the distribution of governance tokens has in the past skewed heavily towards founders and early adopters, thus concentrating decision-making power in the hands of a few holders (sometimes referred to as token whales). This raises concerns about fair representation of all participants. Decision-making processes in DAOs are evolving in the pursuit of fair representation and to address market demands for adaptable and transparent governance.

56. Equally important to improving DAO governance is the evolution of mechanisms to resolve disputes among participants regarding the decision-making process. Multi-tiered resolution mechanisms, combining community mediation with on-chain arbitration, have become a feature of robust DAO governance. It is however also important that such mechanisms would seamlessly interact with other relevant laws to ensure recognition and enforcement of the outcome of the dispute resolution process in domestic and cross-jurisdictional contexts.

Identification of token holders

57. Identifying DAO participants is necessary to allocate roles and liability, but *pseudonymity* allows DAO participants to operate under the publicly available cryptographic hash of their wallet address. While *pseudonymity* promotes privacy and inclusivity, it can also introduce operational risks regarding lack of accountability, governance and security as in many cases identifying the entities involved may be difficult.

58. The creation and use of a uniform identification framework linking electronic signatures to governance token ownership could address several core governance and accountability challenges inherent in decentralized organizations. The identification framework for members, developers and operators within a DAO could find appropriate treatment in laws on identity management of general application based on the UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services (MLIT).[9]

59. In the context of DAOs, verifiable *identity credentials* can be used to confirm a member's identity, qualifications or reputation. By implementing verifiable credentials, DAOs could ensure that only qualified individuals participate in governance and decision-making processes. These credentials can be stored off-chain to protect privacy and linked to on-chain activities through cryptographic proofs.

2. The legal framework for DAOs

60. One of the challenges arising from the use of a DAO is defining rights and obligations of each party, especially when using public permissionless distributed ledgers, because of the uncertainty in their legal status. A DAO's uncertain legal status hinders interaction with external parties such as service providers, investors and regulatory bodies.[10]

61. Some DAO participants may set up traditional corporations to carry out commercial transactions outside the DAO, which are called off-chain transactions. This means that a traditional corporation will coexist with the DAO. In other cases, DAOs may get legal personality by registering under dedicated laws that typically allow DAOs to limit their liability like a limited liability company. This, however, does not automatically entail that such legal status will be recognized in other jurisdictions.

[9] *UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services*, United Nations publication, Sales No. E.23.V.10.

[10] For additional information on the legal status of DAOs, including dedicated legislation and case law, see A/CN.9/1225. At its fifty-eighth session, in 2025, UNCITRAL has authorized exploratory work on legal issues relating to the use of decentralized autonomous organizations in trade (A/80/17, para. 261).

62. In some jurisdictions, plaintiffs have sought redress by alleging unlimited personal liability of the participants in the DAO. However, from a practical perspective, pursuing individual members of a DAO may be a lengthy and difficult process, especially if the DAO's members are identified only with pseudonyms and are located in multiple jurisdictions.

63. Uncertainty in the legal status of DAOs and their operations reverberates in the application of all areas of law. For instance, the application of existing insolvency laws may not accommodate the operational and technological realities of DLT. Moreover, a DAO may not be able to file for insolvency proceedings as this presupposes legal personality.

C. Which legal issues may arise when using distributed ledger technology?

64. DLT may offer significant benefits to its users. However, its features may also raise peculiar legal issues, which may be considered at a general level and with regard to specific DLT applications.

1. Contract automation

65. The broad availability of data and other advances in technology have led to a significant increase in the automation of the exchange of electronic communications. Contract automation allows, among other things, concluding and performing many contracts simultaneously at limited cost and adjusting the terms of contracts to evolving market conditions in real time. Metadata and data generated from objects through an *oracle* may be used as a condition for triggering the automated execution of contracts.[11]

66. Commercial operators should consider carefully if contract automation can accommodate all the conditions and circumstances relevant to their dealings. For example, clauses that require consideration of specific circumstances, such as force majeure and compensation clauses, may not be easily transposed in code for automated execution. Considering the number of conditions to be clarified and the complexity of the scenarios, contractual parties may prefer not to automate such clauses. On the other hand, clauses referring to the foreseeability of an event may benefit from the availability of large data sets on the occurrence of that event, thus making the event more accurately predictable and ultimately facilitating risk allocation.

[11] Examples include the triggering of the DLT-based automated contract when certain parameters, for example, geolocation of a ship or due date for payment, are achieved.

67. Service providers often promote the use of DLT in contract automation by referring to smart contracts. Because of information persistence, neither party may easily alter unilaterally the scripts coded on a distributed ledger. The use of DLT may thus increase the confidence in the automated execution of contracts.

68. On the other hand, DLT immutability may pose challenges when the law requires the inclusion of software that stops the automated execution of the contract (known as a *kill switch*) to prevent undesirable effects, for example, placing an excessive demand on a consumer.[12] Commercial operators should carefully consider whether applicable law requires such software and if technical solutions fully address legal requirements.

69. For the use of the MLAC in contract automation and smart contracts, see paras. 118–119 below.

2. Liability for incorrect information

70. An aspect of liability and risk allocation pertains to instances where the information on the distributed ledger is inaccurate, for instance due to a good faith mistake or fraudulent behaviour. This may happen at the development stage (for example, inserting malicious code while deploying the distributed ledger) or during information input (for example, information known to be inaccurate was entered). The liability for recording inaccurate or false information lies with the person providing the information or on whose behalf the information was provided.

71. As *persistence of information* may hinder entering corrections, commercial operators should ensure that the data stored on the distributed ledger is correct. They should consider measures that may prevent incorrect data input, for example, by broadcasting the data to be entered within the network or establishing internal guidelines to confirm data accuracy and restrictions on data entry. Moreover, commercial operators permitting users, in particular third parties, to input information in their private permissioned distributed ledger should limit contractually, to the extent possible, their liability with respect to those users.

[12] See, for example, article 36(1)(b) of the Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonized rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), OJ L, 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj, requiring (also) DLT-based automated contracts to comply with one of the essential requirements of safe termination and interruption, that is "to ensure that a mechanism exists to terminate the continued execution of transactions and that the smart contract includes internal functions which can reset or instruct the contract to stop or interrupt the operation, in particular to avoid future accidental executions".

Case study: Right to amend information stored incorrectly

Information stored on a distributed ledger may need to be modified, including at the request of a third party. However, because of *persistence of information,* it may be difficult to amend stored information that is incorrect or to update or change data that is no longer relevant or accurate. The workaround solution would be setting up pre-defined governance rules and reducing centralization in favour of control over data. Moreover, software code may allow revising or deleting of data at the user's request.

3. Data privacy and protection

72. Numerous States have enacted data privacy and protection laws that are applicable to DLT-based applications. For instance, the EU General Data Protection Regulation (GDPR)[13] applies when personal data is involved, including when DLT is used. It has been suggested that a public cryptographic key may be considered personal data under the GDPR given the analogies between public keys and dynamic IP addresses.[14]

73. Certain data protection and privacy laws require that data be processed lawfully, transparently and for specific purposes, and that a "controller" or "processor" as defined by the law, could be held accountable for violations. In other cases, the definition is less explicit, focusing instead on the right to access, correct and delete personal data while relying on the concept of a "business operator" as the data controller.

74. DLT's decentralized nature and features like *persistence of information* pose peculiar challenges in ensuring compliance with those laws. For example, the personal information of a person resident in one jurisdiction could be stored in a different jurisdiction, and the place of storage may vary regularly or may not be determinable. Moreover, it is unclear how certain distributed ledgers would practically achieve accountability, transparency and purpose specification as the absence of a clearly identifiable central administrator makes it difficult to pinpoint a data controller.

75. Additionally, distributed ledgers may struggle to meet informed consent and clarity requirements for data processing purposes. Similar challenges arise when data

[13] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, pp. 1–88, ELI: http://data.europa.eu/eli/reg/2016/679/oj.

[14] For the application of GDPR to dynamic IP addresses, see European Court of Justice, 19 October 2016, *Patrick Breyer v. Bundesrepublik Deutschland*, ECLI:EU:C:2016:779.

protection regimes require data controllers to ensure that data subjects are informed, lacking a single identifiable party that could act as the primary point of contact for data subjects.

76. Detailed rules govern the cross-border transfer of personal data in different jurisdictions. This leads to another question. If the recipient is also a participant in a blockchain network, how is this to be practically achieved? Distributed ledgers often operate on a global level, their users being in multiple jurisdictions. Therefore, the difficulty of transferring data due to the lack of harmonization between legal regimes on cross-border data transfers is compounded by data being on-chain.

77. When using distributed ledgers, commercial operators should consider whether personal data will be stored on the distributed ledger and comply with applicable data privacy and protection laws. As the distributed ledger developer, operator and user can be located across multiple jurisdictions, clauses should be inserted in the contractual agreements to ensure compliance with all relevant data privacy and protection laws.

Case study: Right to be forgotten and right to deletion

The *persistence of information* stored in DLT may pose challenges in relation to compliance with certain rights such as the *right to be forgotten* and the *right to deletion*. These issues become even more relevant when the information in question is highly sensitive personal data, such as healthcare records or biometric information.

Generally, data protection regimes require that data subjects have the right to request the deletion of their personal data, which may be challenging when considering the *persistence of information* recorded on a distributed ledger. The application of the principle of data minimization could overcome some of these challenges. Furthermore, as noted (para. 74 above), it may be difficult to identify a data controller or other entity responsible, also for enforcing the *right to be forgotten* and the *right to deletion*.

A possible solution leverages the fact that DLT developers and administrators may agree to remove certain data from private permissioned ledgers. However, this solution does not address data deletion in public permissionless ledgers. Another solution is the storage of personal data in a database that is not on the distributed ledger. Such a solution does not however solve in full the problem of the *right to deletion*, and it may increase costs.

Alternatively, commercial operators may consider encrypting and anonymizing data so that the data is not easily associated with an individual. If such data is lost and subsequently found by an individual who is not in possession of the decryption key, encryption and anonymization will render access to the data useless.

However, technical measures currently available may not always suffice to fully protect personal data. Moreover, preserving confidentiality of the transaction should not hinder

its auditability. When these *privacy-enhancing features* may not be implemented, for example, because of the use of a public permissionless ledger, data minimization in processing information across the network should be pursued. Technical solutions are being developed to address the issue based on fully homomorphic encryption, which allows computation of encrypted data without the need to decrypt it first.

4. Identification and pseudonymity

78. As noted (para. 12 above), the use of pseudonyms is common in DLT systems. Certain laws recognize and accommodate the use of pseudonyms in electronic transactions by indicating that *pseudonymity* should not be prohibited if it complies with legal and regulatory requirements.[15] This approach preserves the flexibility of *pseudonymity* while allowing identity verification as required.

79. A party using a pseudonym may be identified by using factual elements. For instance, with regard to the identification requirement set in article 9 of the MLETR for electronic signatures used in electronic transferable records, the "identification, and the possibility of linking pseudonym and real name, including based on factual elements to be found outside distributed ledger systems, could satisfy the requirement to identify the signatory" (MLETR Explanatory Note, para. 78).

80. While *pseudonymity* may not necessarily impede the identification of the party, it may hinder it, particularly if the law requires the use of a certain method or procedure to identify the party, or the fulfilment of a specific *level of assurance* of the asserted identity. Moreover, the regulation of certain business fields requires identification of the parties. In particular, operating under pseudonyms may hinder compliance with anti-money-laundering (AML) and know-your-customer (KYC) requirements. This may limit the use of DLT applications.

81. Commercial operators should verify whether identification obligations apply to their business (for example, KYC and AML requirements for trading digital assets, or personal data anonymization requirements). Technical solutions, such as selective or minimal disclosure techniques, may achieve satisfactory identification. Additional precautions such as anomaly and fraud detection measures may be needed, for instance to avoid insider trading of digital assets stored on the ledger. Anomaly and fraud detection mechanisms include analysing data (either statistically or using machine learning) to detect any anomalies in activities and patterns.

[15] See, for example, article 5 of the eIDAS Regulation, as amended: "Without prejudice to specific rules of Union or national law requiring users to identify themselves or to the legal effect given to pseudonyms under national law, the use of pseudonyms that are chosen by the user shall not be prohibited".

Use case: Service of documents to pseudonym addresses

In case of litigation, it is necessary to inform concerned parties of the proceedings. A specific challenge may arise when legal notices and documents must be served to a pseudonymous address that is the only known address of that party. This need typically arises in conjunction with loss of control on digital assets due to theft or fraud.

Procedural law requires carrying out service with mechanisms identified by the law or the judge. In certain jurisdictions the law is more flexible on such matters. For instance, some courts have authorized service of documents via social media. Other courts have permitted the delivery of NFTs in a wallet (called "airdrop") for service of documents to pseudonymous addresses.[a] The NFT contains a link to download the document and is sent to the wallet address where the plaintiff has tracked the stolen or lost digital asset.

When service is effected by NFT, the serving party may wish to take adequate measures to ensure confidentiality of the document served.[b] Service with NFT may also provide information on the time of the delivery of the NFT, its opening by the recipient and the access to the served document stored in the distributed ledger.[c] Such service may also confirm whether the document was accessed by a physical person or by a bot. This information is important to ensure compliance of the service method with procedural law.

However, in other jurisdictions the use of such mechanisms for service of documents may be regarded as a violation of fundamental rights.[d] Moreover, the compatibility of such mechanisms with applicable treaties, such as the Hague Convention on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters,[e] may need to be verified.

[a] *LCX Ag v. 1.274M U.S. Dollar Coin*, No. 154644/2022, 2022 WL 3585277 (N.Y. Sup. Ct., 21 August 2022); *Jones v. Persons Unknown* [2022] EWCH 2543 (Comm); *Benjamin Arthur Bowen v. Xingzhao Li* (Case No. 23-cv-20399) (S.D. Fla. 2023, 3 March 2023); *D'Aloia v. Binance Holdings & Others* [2022] EWHC 1723 (Ch).

[b] In *Osbourne v. Persons Unknown* Category A & Ors [2023] EWHC 39 (KB) the judge, noting that "the NFTs used to effect service would be open to the public and the hyperlinks contained in them could be used by anyone to view the documents served", authorized the service of redacted documents by NFT conditional on the use of redactions approved by the court and the defendants being offered access to unredacted versions of the documents (para. 49).

[c] In re Celsius Network LLC, Case No. 22-10964 (MG) (Bankr. S.D.N.Y. 24 October 2024).

[d] In general, on due process in online proceedings, see *X v. Y*, Gerechtshof Amsterdam, 29 January 2019, ECLI:NL:GHAMS:2019:192, CLOUT Case 1921.

[e] United Nations, *Treaty Series*, vol. 658, no. 9432, p. 163.

5. Digital assets

82. The legal treatment of digital assets has attracted significant attention. While any data has some value regardless of the technology used, and therefore may be considered an asset, the legal notion of "digital asset" often refers to storage and

transfer of value by using DLT. Similarly, in business practice digital assets are often tied to the use of DLT.

83. Even under a technology neutral approach, different definitions of "digital assets" exist. One definition focuses on the ability to control and transfer the digital asset. According to Principle 2 of the *UNIDROIT Principles on Digital Assets and Private Law* (DAPL), which is in turn inspired by the definition of "controllable electronic record" contained in Section 12-102 of the Uniform Commercial Code (UCC) of the United States of America, "'digital asset' means an electronic record which is capable of being subject to control". Other definitions of "digital asset" focus on what the asset "represents", that is the rights that the digital asset incorporates.[16]

84. The Taxonomy recognizes the lack of consensus on the definition of digital assets; however, it provides that, in its ordinary meaning, the term "digital asset" connotes a collection of data, stored electronically, that is of use or value (Taxonomy, para. 82). Some assets may fall under the definition of digital asset but also under other definitions that are legally relevant, for example, that of an electronic trade document. In those cases, it is particularly important to determine which legal regime shall prevail.

85. Laws have been drafted on the regime applicable to digital assets.[17] These laws define how digital assets may be issued and transferred. They may also specify if digital assets may be the subject of proprietary rights (see Principle 3(1) of the DAPL). While these laws may be technology neutral, digital assets issued on DLT are particularly relevant for their application. It is in any case important to note when the law uses a technology neutral definition of "digital asset", and when it refers to the use of DLT only.

86. Another legislative approach is based on the definition of technical requirements that must be met in order to issue digital assets.[18] Those technical requirements aim at ensuring that the digital asset is controlled and transferred according to the will of its holder as reflected in contractual agreements. One benefit of this approach may lie in the ability to predetermine the requirements that systems and services should meet

[16] See the definition of "digital asset" as "asset that exists only in digital form or which is the digital representation of another asset" found in International Organization for Standardization, *ISO 22739:2024 Blockchain and distributed ledger technologies – Vocabulary* (Geneva, 2024), 3.20.

[17] In the United States of America, UCC Article 12; in the United Arab Emirates, Dubai International Financial Centre, Digital Assets Law, Law No. 2 of 2024; and the DAPL as a uniform model. See also United Kingdom, Law Commission of England and Wales, *Digital assets as personal property: Supplemental report and draft Bill*, Law Com No 416 (London, 2024).

[18] In Switzerland, Loi fédérale sur l'adaptation du droit fédéral aux développements de la technologie des registres électroniques distribués du 25 septembre 2020; in Liechtenstein, Token & Trustworthy Technology Service Provider Act of 3 October 2019 (Token und VT-Dienstleister-Gesetz).

to be presumed reliable, as such presumption may reinforce the confidence of commercial operators in using those systems and services.

87. Regulatory frameworks for digital assets are also emerging. In Europe, besides early regulations adopted by Liechtenstein and Switzerland, the EU Markets in Crypto-Assets Regulation (MiCA)[19] establishes guidelines for digital assets. Across Asia, countries such as China, Japan, the Republic of Korea[20] and Singapore[21] are implementing policies to manage digital assets, with Singapore providing one of the most comprehensive frameworks for blockchain innovation and digital asset management. In the Middle East, among other jurisdictions, Dubai, an emirate in the United Arab Emirates,[22] is offering guidance on digital assets regulation. The United States of America has also adopted legislation.[23]

88. From a practical perspective, commercial operators who decide to use digital assets should choose or otherwise identify the applicable law mindful of implications. In particular, they should safeguard the application of other laws, such as laws applicable to commercial documents and to money, and comply with all applicable regulations.

Tokenization

89. Tokenization is the process of linking physical or intangible assets and digital tokens, which are a type of digital asset recorded on a distributed ledger. These tokens represent ownership, contractual rights or other value. The rapid growth of the digital economy and the emergence of DLT technology led to suggestions that any asset may be tokenized.

90. Tokenization serves as a bridge between the physical economy and the digital economy, carrying significant legal and regulatory implications for financial markets, financial inclusion and individual data rights. It may reduce long-standing barriers to investment – such as high minimum thresholds or inherent asset illiquidity – possibly facilitating broader access to diverse asset classes and promoting a more inclusive financial ecosystem.

[19] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937, OJ L 150, 9.6.2023, pp. 40–205, ELI: http://data.europa.eu/eli/reg/2023/1114/oj.

[20] Act on the Protection of Virtual Asset Users, Act No. 19563, of 18 July 2023.

[21] Ministry of Finance of Singapore, Virtual Assets Risk Assessment Report Singapore 2024.

[22] Dubai Virtual Assets Regulatory Authority, Virtual Assets and Related Activities Regulations 2023.

[23] Public Law 119–27, Guiding and Establishing National Innovation for U.S. Stablecoins Act or the "GENIUS Act" (18 July 2025).

91. In this context, tokens can be grouped into three main categories:

- The first category is related to real-world assets (RWA), such as bills of lading, warehouse receipts and rights in real estate, so that tokens are directly tied to tangible goods or title to rights. These are commercial documents in electronic form issued as tokens, and the law of those commercial documents should apply. Electronic transferable records compliant with the MLETR, electronic warehouse receipts compliant with the UNCITRAL–UNIDROIT Model Law on Warehouse Receipts (MLWR)[24] and electronic negotiable cargo documents issued under the United Nations Convention on Negotiable Cargo Documents (the "NCD Convention")[25] may be issued as RWA tokens;
- The second category includes money and money-like assets like *central bank digital currencies* (CBDCs), *stablecoins* and tokenized cash equivalents, which facilitate payment systems and financial inclusion. These digital assets may be further tokenized as financial products such as exchange-traded funds (ETFs) and money market funds that utilize *stablecoins* or other digital assets. The integration of *stablecoins* into regulated financial products such as ETFs or money market funds aims to enable continuous trading, reduce transaction costs and improve liquidity; and
- The third category pertains to financial products and intellectual property rights, and includes tokenized securities, related ETFs and NFTs representing creative works.

92. The main distinction lies in whether the tokens are linked to RWA or exist independently, such as in the case of cryptocurrencies. This distinction significantly impacts legal status as tokens linked to RWA rely on underlying legal frameworks for rights allocation and dispute resolution, while tokens that are not tethered to RWA may lack a similar legal framework, posing regulatory challenges and greater risk exposure.

93. The HCCH Experts' Group on Digital Tokens is conducting work on private international law (PIL) questions raised by tokens, including the study of questions of applicable law, jurisdiction, recognition and enforcement and international cooperation mechanisms.[26] The work of the Experts' Group focuses on the examination of specific tokenization use cases that may have implications for PIL based on the cross-border decentralized nature of DLT systems and the *pseudonymity* of users.

[24] *UNCITRAL–UNIDROIT Model Law on Warehouse Receipts*, United Nations publication, Sales No. E.25.V.3.

[25] A/80/17, Annex I.

[26] In March 2025, the HCCH Council on General Affairs and Policy adopted Conclusion and Decision No. 15, which "mandated the establishment of an Experts' Group to study the PIL issues raised by digital tokens, subject to available resources". For further information, see HCCH Preliminary Document No. 4 of November 2024, available on the HCCH website at www.hcch.net under "Governance" then "Council on General Affairs and Policy".

Electronic transferable records

94. Electronic transferable records, as defined in the MLETR, may be issued using DLT-based systems and services. For instance, in China the Standing Committee of the Shanghai Municipality adopted a set of legal provisions enabling the use of blockchain-based electronic trade documents in the Lingang Pilot Free Trade Zone that incorporate the principles of the MLETR, and the application of those legal provisions was eventually extended to other special economic zones. Those records are transferable documents and instruments in electronic form and, as such, the law of those documents and instruments applies together with the rules contained in the MLETR. In the classification above, tokenized electronic transferable records are RWA tokens.

95. The Explanatory Note to the MLETR provides specific guidance on selected DLT-related issues. For instance, consent to the use of an electronic transferable record in systems that lack a centralized operator may be implicit and inferred by circumstances such as exercise of control of the record or performance of the obligation contained in the record (MLETR Explanatory Note, para. 66). Moreover, where pseudonyms are used, the requirement to identify the person in control may be satisfied by linking pseudonym and name (MLETR Explanatory Note, para. 117).

96. The HCCH Experts' Group on Digital Tokens (see para. 93 above) has identified the consideration of PIL issues relating to data and objects falling under the MLETR as one priority use case in the context of the HCCH Digital Tokens Project and is advancing the study of this use case in coordination with UNCITRAL.[27]

97. Similar considerations apply to the issuance of electronic transferable records under a law that does not foresee a functional equivalence approach but legally enables the use of those records in electronic form only. Likewise, those considerations apply to electronic transferable records issued under a law that enables the use of both paper-based and electronic documents by adopting a medium-neutral approach. The MLWR and the United Nations Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea (New York, 2008) (the "Rotterdam Rules")[28] are examples of laws adopting a medium-neutral approach.

[27] Other priority use cases studied by the Experts' Group are bitcoin, *stablecoins* and agrotokens. Secondary priority use cases include healthcare tokens, NFTs, including *soulbound tokens*, governance tokens and DAOs, and staked tokens and consensus mechanisms.

[28] General Assembly resolution 63/122, annex.

Cryptocurrencies

98. Digital assets used to transfer value are often referred to as cryptocurrencies.[29] Cryptocurrencies may have a market value, if sufficiently liquid to be traded in dedicated markets (*crypto-exchanges*). Some cryptocurrencies, called *stablecoins*, link their value to *fiat* money or other assets to mitigate volatility.

99. At times, some States have declared cryptocurrencies legal tender beside the national currency. This has raised novel questions, for instance on the exchange rate between the pre-existing currency and the cryptocurrency and, more generally, on the impact on monetary policy.

100. Challenges arising from the use of cryptocurrencies are of legal, regulatory and commercial nature. The legal qualification of a cryptocurrency, including the applicable regulatory regime, depends on its features. Regulators may consider cryptocurrencies as commodities, securities or both.[30] Payment services carried out using cryptocurrencies are subject to payments law and regulation.

101. While cryptocurrencies may be accepted as a means of payment, it remains doubtful whether they could be assimilated with *fiat* money. Such assimilation has important legal consequences with regard to performance of the obligation to pay, setting off of monetary obligations and the characterization of certain contracts, for example, as sale or barter contracts (see Taxonomy, paras. 108–110).

102. Another unsettled matter relates to the ability to classify cryptocurrencies as property. In those jurisdictions where this is possible, cryptocurrency holders may use proprietary remedies, for example, the freezing of an asset,[31] to recover lost or stolen cryptocurrencies.

103. From a business perspective, the fact that transfer of value through cryptocurrencies does not require the involvement of intermediaries may reduce transaction time and costs, including exchange rate fees. On the other hand, the irreversibility of the transaction may prevent chargebacks, which occur with other payment instruments, especially credit cards used for refunds in transactions with consumers.

---

[29] The original goal behind the creation of bitcoin was the ability to enable decentralized payments.

[30] In some cases, cryptocurrencies may be qualified as commercial documents. For instance, a commoditized stablecoin (that is a stablecoin whose value is linked to a specific commodity) may be qualified as a warehouse receipt if the commodity is identified and stored in a warehouse (as opposed to a commodity price index) and the other legal requirements of a warehouse receipt are met.

[31] For instance, in *AA v. Persons Unknown* [2019] EWHC 3556 (Comm), an English court allowed for a proprietary injunction for bitcoins in connection with a ransom payment. Civil asset tracing and recovery in insolvency proceedings, including with regard to digital assets, is a topic dealt with in a dedicated UNCITRAL workstream (see A/80/17, paras. 129–136).

104. Cryptocurrencies may be risky and speculative. Yet, when national currencies are highly volatile, including due to hyperinflation, or restrictions on cross-border payments are in place, cryptocurrencies may be seen as a more stable and effective form of value transfer than traditional payment methods.

105. Commercial operators wishing to use cryptocurrencies for payments may consider using different *crypto-exchanges* to mitigate risks related to hacking and default of a crypto-exchange. They may also diversify cryptocurrencies to counter challenges if the exchange or the currency proves to be problematic, for instance, due to an excessive drop in value or scarce liquidity. Also, if the applicable law classifies cryptocurrencies as property, the related tax regime would apply, including capital gains tax. Finally, commercial operators should always ensure that the payment services used comply with applicable law and regulations, which may be particularly detailed.

Central Bank Digital Currencies and payment systems

106. CBDCs are defined as *fiat* money issued in electronic form. As such, they are issued only by central banks and are different in nature from cryptocurrencies.[32] Pilot projects with CBDCs, which may or may not involve the use of DLT,[33] may concern both the wholesale and the retail use of CBDCs.[34] The HCCH is conducting work on the applicable law and jurisdiction issues raised by the cross-border use and transfers of CBDCs.

107. Early applications of DLT have pursued transfer of value in a decentralized manner by creating cryptocurrencies. However, distributed ledgers may also be used to transfer value with CBDCs and *fiat* money recorded on ledgers. In general, benefits associated with the general features of DLT, such as *persistence of information*, apply regardless of the unit of value used.

[32] The International Monetary Fund has released a *Central Bank Digital Currency Virtual Handbook*, which provides information on policymakers' most frequently asked questions on CBDCs. It also provides users with a framework to explore CBDCs and a CBDC product development chapter. The Handbook is available online.

[33] For example, Project mBridge of the Bank for International Settlements Innovation Hub uses a dedicated distributed ledger for multi-CBDC cross-border payments.

[34] Wholesale *fiat* money may already be created only in electronic form as an entry in a ledger. Once the money is transferred to commercial banks, those banks have a debt towards the central bank that created the money on the ledger.

Part three.

Application of UNCITRAL Texts on Electronic Commerce to Distributed Ledger Technology

108. UNCITRAL texts on electronic commerce may significantly contribute to legal predictability of the use of DLT in trade, especially with regard to issues arising between a commercial operator and its clients during the delivery of DLT-based services.

A. Application of the fundamental principles underlying UNCITRAL texts on electronic commerce to distributed ledger technology

1. Technology neutrality

109. The principle of technology neutrality is a cornerstone of UNCITRAL electronic commerce texts. Technology neutrality mandates the adoption of legal provisions that are neutral with respect to technologies, methods and products used. This means that when technology advances further legislative work is not required as technology neutral laws already accommodate future developments. Because of technology neutrality, UNCITRAL texts enable the use of DLT.

110. The definition of "data message", which is used as the building block to refer to all information in electronic form, ensures UNCITRAL texts apply to all available technologies.[35] For instance, article 4, subparagraph (b) of the United Nations Convention on the Use of Electronic Communications in International Contracts (ECC)[36] defines "electronic communication" as "any communication that the parties make by means of data messages".

111. Building on a similar notion, article 2 of the MLETR defines "electronic record" as "information generated, communicated, received or stored by electronic means".

[35] See, for example, the definition contained in article 1, subparagraph 1(b) MLAC: "'Data message' means information generated, sent, received or stored by electronic, magnetic, optical or similar means".

[36] United Nations, *Treaty Series*, vol. 2898, no. 50525, p. 3.

Mindful of the composite nature of electronic records stored on DLT, the article clarifies that the notion of electronic record encompasses "all information logically associated with or otherwise linked together so as to become part of the record, whether generated contemporaneously or not". To sum up, data messages and electronic records, as defined in UNCITRAL texts, may be stored in distributed ledgers.

2. Legal recognition and effect

112. Likewise, provisions contained in UNCITRAL texts that give general legal recognition and effect to the use of electronic means apply also to the use of DLT. Besides operating at the national level, those provisions facilitate, to the extent possible, cross-border recognition of electronic communications and documents. The fact that UNCITRAL texts provide for legal recognition regardless of the place of origin or use of electronic means (for example, art. 19, para. 1 of the MLETR) may facilitate the use of distributed ledgers that, by their nature, may be located in multiple jurisdictions.

113. One limit to the legal recognition of data messages stored in distributed ledgers may come from national law requiring the use of national encryption standards and schemes. As DLT is based on the use of encryption technologies, those laws may limit the ability to give legal recognition to the use of distributed ledgers that are based on other standards and schemes, including international ones.

3. Functional equivalence

114. The principle of functional equivalence enables the satisfaction of paper-based form requirements with the use of electronic means. Besides requiring the fulfilment of certain criteria, functional equivalence presupposes the use of reliable methods to achieve the intended purpose. Features of DLT such as *persistence of information* and, when using NFTs, assurance of singularity (see para. 117 below) may facilitate satisfying functional equivalence requirements contained in UNCITRAL texts (see also Taxonomy, para. 201).

115. Information persistence in DLT may be used to implement the concept of "integrity" under UNCITRAL electronic commerce texts, which is relevant for certain functional equivalence rules:

- Under article 8 of the UNCITRAL Model Law on Electronic Commerce with Guide to Enactment (MLEC),[37] integrity is one of the functions that a

[37] *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment*, United Nations publication, Sales No. E.99.V.4.

data message must fulfil in order to meet a legal requirement that the information be presented or retained in its original form. The function is fulfilled if the information remains "complete and unaltered" from the time it was first generated in its final form, apart from the addition of any endorsement and any change that arises in the normal course of communication, storage and display. The same requirement is contained in article 9, paragraph 4 of the ECC. Methods that use DLT may provide a higher level of reliability with regard to assurance of integrity;

- Under article 10 of the MLETR, integrity is one of the functions that an electronic transferable record must fulfil to be legally equivalent to a paper-based transferable document or instrument; and
- Article 6, subparagraph 3(d) of the UNCITRAL Model Law on Electronic Signatures with Guide to Enactment[38] acknowledges that certain types of electronic signatures may detect any alteration to the signed information. This function is typically fulfilled by electronic signatures that use cryptographic techniques and therefore may be found in DLT systems. In a similar vein, article 17 of the MLIT prescribes integrity as one of the functions of electronic seals, and article 20 of the MLIT does the same for electronic registered delivery services.

116. Similarly, *persistence of information* may assist in satisfying other requirements contained in UNCITRAL texts. For instance:

- Article 9 of the MLEC indicates that, in assessing the evidential weight of a data message, regard shall be had, among other circumstances, to the reliability of the manner in which the integrity of the information was maintained; and
- Article 19 of the MLIT requires that the archived data message be retained in the format in which it was generated, sent or received, or in another format that can be demonstrated to detect any alteration to the data message after that time and date, apart from the addition of any change that arises in the normal course of communication, storage and display.

117. Article 10, subparagraph 1(b)(i) of the MLETR requires singularity of the electronic transferable records, that is the reliable assurance that the electronic trade document exists only in one electronic record. NFTs are a specific application of DLT that may offer a higher *level of assurance* of singularity of a digital asset because of their technical specifications. Thus, the use of NFTs may facilitate fulfilment of the singularity requirement of electronic transferable records. DLT is being used by several

[38] *UNCITRAL Model Law on Electronic Signatures with Guide to Enactment*, United Nations publication, Sales No. E.02.V.8.

providers of electronic trade documents that operate in compliance with the MLETR and a similar use with regard to documents issued under the MLWR and the NCD Convention is foreseeable.

B. Use of distributed ledger technology in electronic contracting

118. Cognizant that contract automation may take place with different methods and technologies, UNCITRAL has prepared the MLAC to deal with legal aspects of contract automation on a technology neutral basis. Therefore, the MLAC applies also to automation based on DLT. Contractual parties who wish to have legal certainty on the use of automated contracts may choose as applicable law the law of a jurisdiction that has enacted the MLAC or incorporate the provisions of the MLAC as contractual terms.

119. Legal issues treated in the MLAC include legal recognition of automated contracting and of contracts in computer code and the use of dynamic information in automated contracting (respectively, arts. 5 and 6 of the MLAC) and attribution of actions carried out by automated systems (art. 7 of the MLAC). Moreover, the algorithm used for contract automation may operate in a non-deterministic manner and carry out actions that are not expected by the party to whom the action is attributed, which may lead to the unintended effect of binding that party to such unexpected action. Article 8 of the MLAC offers a rule for dealing with such issues.

1. Electronic signatures

120. From a technical perspective, digital signatures, that is signatures based on cryptography, are a foundational component of DLT networks, serving as the primary means by which users authenticate and authorize transactions, including those executed by automated means. These signatures verify the identity of participants and establish within a decentralized system the validity of the transactions and the integrity of their content, making them indispensable for user trust and network security. As the adoption of DLT grows across sectors, the demand for reliable electronic signatures increases, underscoring their role as a critical market requirement.

121. From a legal perspective, DLT-based electronic signatures may be qualified as a trust service used to provide data quality assurance (art. 16 of the MLIT). They may also be used to identify the signatory and to express its intent with regard to the signed message, thus fulfilling the requirements set in UNCITRAL texts for functional equivalence between electronic and handwritten signatures. Conversely, the principles

of technology neutrality and non-discrimination against the use of electronic means underpinning UNCITRAL texts also apply to electronic signatures based on the use of DLT, which are therefore legally recognized.

122. As noted (para. 113 above), some laws may require the exclusive use of specific technologies or services (such as "qualified signatures" or "digital signatures") and may impose the use of certain technical standards and national providers. These laws, which are not technology neutral, may prevent the recognition of foreign or otherwise non-compliant electronic signatures, including DLT-based ones. Such laws may also be incompatible with provisions in trade agreements that mandate the use of technology neutral electronic signature or electronic authentication methods.

Use case: Multi-party signatures

A specific application of electronic signatures in distributed ledgers pertains to the use of *multi-signature ("multisig") wallets*. This technology is used when the consent of multiple parties, expressed in affixing each party's electronic signatures, is required to authorize a transaction (for example, to release assets from escrow accounts; in public procurement, to open submitted offers and tenders; in arbitration, to sign arbitral awards rendered by a panel, etc.). In this case, the affixation of multiple encryption-based signatures from predetermined addresses may be required to proceed with the transaction.

Multi-signature ("multisig") wallets can benefit from the integration of a cloud computing technique known as Multi-Party Computation (MPC). This technique enhances the privacy and security of electronic signatures by allowing multiple parties to jointly compute a cryptographic signature without disclosing individual private keys. MPC may ensure that each participant's input remains confidential, safeguarding identity and signature details throughout the transaction process.

C. Distributed ledger technology and private international law

123. In general, PIL rules assist in determining the applicable law absent a valid choice of law by the parties. The need for PIL rules in the DLT context may arise due to the multiplicity of jurisdictions possibly involved in the operation and use of DLT, and the difficulty in agreeing on the choice of law, especially in

permissionless DLT systems. Participants in a DLT system can be scattered across multiple jurisdictions.[39]

124. The definition of "information system" as "a system for generating, receiving, storing or otherwise processing data messages" (art. 2, subpara. (f) of the MLEC and art. 4, subpara. (f) of the ECC) encompasses distributed ledgers. However, unlike other technology, DLT has a decentralized nature. The various components of a DLT-based information system may therefore be located in different jurisdictions or may also change location regularly. For this reason, the rule contained in article 6, paragraph 4 of the ECC, indicating that the location of equipment and technology supporting the information system is not necessarily the place of business of a party, may be particularly useful when DLT is used.

125. The decentralized nature of DLT may also pose a challenge to compliance with data localization requirements because it may not permit localization of the distributed ledger system in only one jurisdiction.

[39] The study of PIL issues arising from the use of DLT, including the matters of applicable law, jurisdiction, recognition and enforcement and international cooperation mechanisms, is ongoing at the HCCH under multiple formal Experts' Groups and monitoring projects. For further information, see the HCCH website.

Glossary[40]

Business continuity management: the process of ensuring that an organization can continue to operate in case of a disaster, disruption or unexpected event. This includes identifying potential threats and vulnerabilities, developing and implementing plans to mitigate or prevent those threats, and testing and maintaining those plans to ensure that they are effective.

Central Bank Digital Currencies: *fiat* money in electronic form.

Consensus: an agreement among nodes on how a transaction on the distributed ledger is validated.

Consensus mechanism: the mechanism in which *consensus* is reached. Most common types of *consensus mechanism* are the *proof of work* and *proof of stake* mechanisms.

Cryptographic hash function: an algorithm that takes a string of input and converts it into an output of a fixed size. This output can be stored and later used for verification purposes.

Crypto-exchanges: trading platforms or markets whereby digital assets can be bought and sold, depending on the individual platform's offerings.

Data silo: a pool of data that is normally isolated from certain groups of users and not easily accessible by the same groups of users.

Distributed ledger audit: an audit process to filter dysfunctional or fraudulent codes or identify any potential vulnerabilities or weaknesses in the DLT system.

Identity credentials: the data, or the physical object upon which the data may reside, that a person may present for electronic identification (art. 1(e) of the MLIT).

Kill switch: software that can stop self-execution of automated clauses.

[40] Other publications on this topic contain valuable glossaries: see, for example, International Telecommunication Union (ITU), ITU-T Focus Group on Application of Distributed Ledger Technology (FG DLT) Technical Specification FG DLT D1.1, *Distributed ledger technology terms and definitions* (Geneva, 2019), International Organization for Standardization, *ISO 22739:2024 Blockchain and distributed ledger technologies – Vocabulary* (Geneva, 2024), and the glossary contained in United Kingdom of Great Britain and Northern Ireland, Law Commission of England and Wales, *Decentralised autonomous organisations (DAOs). A scoping paper* (London, 2024).

Level of assurance: in the context of identity management, a "level of assurance" means a designation of the degree of confidence in the identity proofing and electronic identification processes, that is: (a) the degree of confidence in the vetting process used to establish the identity of a subject to whom a credential was issued; and (b) the degree of confidence that the subject using the credential is the subject to whom the credential was issued. The *level of assurance* thus reflects the reliability of methods, processes and technologies used (MLIT Guide to Enactment, para. 160).

Mining: activity in specific consensus mechanisms, such as *proof of work*, which validates ledger records on the distributed ledger. Miners are participants in this activity.

Multi-signature ("multisig") wallets: a service using multiple private keys that allows digital assets to be controlled, stored or transferred.

Node operator: the operator of a computer that is part of a distributed ledger.

Non-fungible tokens: a type of digital asset that is incapable of mutual substitution among individual units.

Oracle: in the context of DLT, a service that supplies information to a distributed ledger using data from outside of a distributed ledger system (ITU-T Technical Specification FG DLT D1.1).

Persistence of information: a feature of distributed ledgers wherein records in the ledger cannot be easily modified or removed once the record is added into the ledger.

Privacy-enhancing features: a set of technology features that support the implementation and harmonization of data management regulations by enhancing data minimization and private computation.

Proof of stake: a type of *consensus mechanism* for validating a record. In *proof of stake*, validators are selected at random after they have put for stake a certain amount of digital assets. When a specific number of validators has been selected and the validators confirm that the record is accurate, the record becomes part of the distributed ledger.

Proof of work: a type of *consensus mechanism* for validating a record. In *proof of work*, miners (as opposed to validators in *proof of stake*) compete to solve an encryption puzzle. Part of the mechanism requires the miner to prove to the network that the miner has completed the encryption and, when proven, the record is added into the distributed ledger. Miners will normally receive digital assets for successful *mining*.

Pseudonymity: this refers to the use of pseudonymous addresses, which are unique strings of characters generated through a cryptographic process and used to represent persons in distributed ledger systems. Pseudonymous addresses may be linked to a physical or legal person and therefore do not ensure anonymity.

Right to deletion: the right of an individual to request an organization or enterprise to delete the personal data of the said individual.

Right to be forgotten: similar to the *right to deletion*, the *right to be forgotten* is the right of an individual to request an organization or enterprise to delete the personal data of the said individual, with an additional requirement of ensuring third parties do not refer or link to such personal data.

Service level management: the process of defining, agreeing and measuring the performance and quality of services that an organization provides to its customers. This includes setting service level targets, monitoring service levels and taking corrective action when necessary to ensure that service levels are being met.

Smart contract: from a technical perspective, smart contracts are self-executing computer code, also called "persistent scripts". When legally relevant, they are automated contractual clauses that execute certain actions once predetermined conditions are met.[41]

Soulbound tokens: these tokens are non-fungible, non-transferable tokens that contain attributes relevant to determining the identity of an entity.

Stablecoins: a type of digital asset whose value is pegged to another asset. This other asset can be either *fiat* money, commodities or other digital assets.

[41] See also the comment in the Taxonomy, para. 33: "At the very most, a 'smart contract' is a program used to perform a contract in an automated manner. At the very least, it is a program used to perform a task in an automated manner without any connection to a contract"; and the definition contained in the European Law Institute *Principles on Blockchain Technology, Smart Contracts and Consumer Protection* (Vienna, 2018): "Computer programme that, upon the occurrence of pre-defined conditions, runs automatically and executes pre-defined actions. A smart contract may or may not be intended to represent terms in a contract in law or be legally recognized. This definition considers smart contracts only in the context of distributed ledger systems. It is recognized that smart contracts are not restricted to distributed ledger systems and the term may have a different meaning in other contexts".

ISBN 978-92-1-157732-7

2516855