United Nations A/CN.9/1175

General Assembly

Distr.: General
29 May 2024

Original: English

United Nations Commission on International Trade Law
Fifty-seventh session
New York, 24 June–12 July 2024

Legal issues relating to the use of distributed ledger technology in trade

Note by the Secretariat

Contents

V.24-09233 (E) 030624 040624

I. Background

1. Mindful that UNCITRAL played a central and coordinating role within the United Nations system in addressing legal issues related to the digital economy and digital trade (A/74/17, para. 211), at its fifty-fifth session, in 2022, the Commission requested the secretariat to prepare 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/77/17, paras. 22(f) and 169). The request of the Commission originated from the preparation of a section on distributed ledger systems in the *Taxonomy of Legal Issues related to the Digital Economy* (the "Taxonomy").

2. At its fifty-sixth session, in 2023, the Commission had before it a note by the secretariat on legal issues relating to the use of distributed ledger technology in trade (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 recently undertaken by the Hague Conference on Private International Law ("HCCH") was noted (A/78/17, paras. 200–202).

3. Accordingly, the Commission requested the secretariat to continue and finalize 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(c)).

4. The present note builds upon and complements the scoping paper by providing additional insight on legal issues relating to the use of distributed ledger technology ("DLT") in trade. It does not provide advice on whether DLT is the appropriate technology for the intended use. This note identifies areas where legal guidance may be found and suggests possible solutions within existing legal instruments. Because of the novelty of DLT, it also identifies areas where no settled legal solution is yet available and, in such cases, it offers a panorama of the evolving landscape. The secretariat intends to further expand this note, including with the help of experts, and to include, in cooperation with the relevant organizations, information on complementary matters such as the interaction between DLT and free trade agreements. In particular, the HCCH holds mandates to work with UNCITRAL and other organisations with relevant expertise on matters relating to the private international law ("PIL") aspects of the digital economy.[1] It is expected that the result of the work of HCCH may be usefully incorporated in the guidance document.

5. This note contains a glossary of technical terms in its annex. The first occurrence of each defined technical term is in italics. The glossary may be further expanded as work on the guidance document progresses.

[1] Conclusions & Decisions of the Council on General Affairs and Policy (CGAP) (C&D of March 2024), No. 11(b), available on the HCCH website at www.hcch.net under "Governance" then "Council on General Affairs and Policy".

II. Content of the guidance document

A. Background information on DLT

6. The Taxonomy 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" (Taxonomy, para. 172).

7. According to another definition, DLT embodies a decentralized database shared across a network of peer-to-peer machines, typically linked via the Internet. It can be architected to allow multiple parties to record and update information. DLT typically harnesses multiple elements such as an information technology infrastructure, an Internet connection, and data. From a technical perspective, these elements generally include a *cryptographic hash* (for instance, of the data in a block), a *consensus mechanism* (e.g. *Proof of Stake*), a platform (such as a layer one protocol) and digital assets (e.g. fungible tokens).

8. Blockchain is a widely known form of DLT. Blockchain utilizes a chain of blocks to archive data. Each block comprises data, such as a transaction log, and a summary – often a cryptographic hash – forming a link to the preceding block. Any alteration in a transaction from an earlier block induces a modification of the associated block's hash, subsequently impacting the hashes of all successive blocks. Thus, modification of information on the blockchain requires amending each subsequent block in chronological order, then broadcasting the updated digital ledger to the network, prior to the addition of a new block to the ledger by another entity. This modification procedure cannot realistically be carried out in sufficiently developed networks. Consequently, the transaction record is persistent. This feature is also known as "immutability".

B. Classification of DLT

9. DLT can be classified based on two key features: public or private ledger, and permissioned or permissionless access to it (Taxonomy, para. 178). The classification is for illustrative purposes and does not reflect the broad variety of solutions available.

10. The public or private nature of distributed ledgers refers to who can participate in developing the DLT system as a *node operator*, i.e. the operator of a computer that is part of the distributed ledger. The term "public ledger" denotes a decentralized system that permits unhindered access. Conversely, a "private ledger" implements restricted access, permitting only a selected group of pre-identified participants.

11. The permissioned or permissionless nature of distributed ledgers refers to whether permission is required prior to participating in the ledger, i.e. 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 are usually in place to allow for identity management.

12. A public permissionless distributed ledger is the most open and decentralized option. In this case, anyone from the public may join the distributed ledger without identity verification and there are usually no administrators to restrict users or participants from accessing, viewing, and recording on the distributed ledger.[2]

[2] Examples of public permissionless distributed ledgers include Bitcoin and Ethereum. Bitcoin's ledger contains the history of every Bitcoin transaction that is available for all to view.

13. A major advantage of a public permissionless distributed ledger is its transparent design, which enhances scalability as new actors do not need to undergo verification by a governing entity. Any actor may access and contribute to such ledger without prior permission or authorization, provided it abides by the self-regulated governance of the network.

14. Key characteristics of public permissionless distributed ledgers include:

(a) Open access: no single administrator controls the network, thus effectively limiting the influence of any single actor on the network;

(b) Open source: the source code is publicly available, and anyone can propose modifications to it;

(c) Transparency: all data on the distributed ledger is publicly visible although *pseudonymity* and other mechanisms may allow some degree of privacy;

(d) Security: 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;

(e) Pseudonymity: actors are identified with pseudonyms at the infrastructure level.

15. In contrast, a private permissioned ledger restricts the number of users and participants in the ledger and requires identification of these participants prior to participating in the ledger. Such ledger is normally created by enterprises and used within these enterprises. This ledger is highly regulated and controlled by the enterprise that created and operates it.

16. Key characteristics of private permissioned distributed ledgers include:

(a) Restricted access: only authorized actors can access and participate in the ledger;

(b) Closed source: code is often not publicly available in the form deployed for the ledger;

(c) Controlled: an entity (organization or group) controls the ledger, so that only selected actors may access the ledger;

(d) Privacy: data may be better protected for privacy and confidentiality purposes due to restricted access to the ledger;

(e) Faster transaction speed: due to a higher level of trust among actors, the consensus protocol can allow for a higher number of transactions per time unit.

17. It is possible, though uncommon, to have 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 are no restrictions in who can participate in the ledger. A private permissionless ledger sets restrictions on who can participate but does not require participants to identify themselves.

C. Features associated with the use of DLT

Persistence of information

18. Persistence of information (or "immutability") is a defining feature of DLT. Consensus is required to modify information stored in the ledger, thereby providing higher assurance of the integrity of that information, namely against unilateral modifications (see para. 8 above). Overall, it is important for enterprises to carefully consider the implications of immutability when implementing DLT in their operations, and to have appropriate measures in place to address issues that may arise.

19. Persistence of information may have far-reaching consequences. For instance, 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), including in special cases such as for consideration of pre-insolvency restructuring.

20. In light of information persistence, it is important to ensure that the data stored on the distributed ledger is correct. Enterprises may consider building in systems that may prevent the incorrect entering of data, e.g. broadcasting of the data to be entered into the distributed ledger within the network or establishing internal guidelines on confirming data accuracy and restrictions to data entry.

21. Depending on the governance and type of DLT, there is a risk that vulnerabilities may be exploited to modify information on the ledger. 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, once a distributed ledger reaches a certain size, the requirement to control more than 50 per cent of the network's hash rate for successful malicious behaviour has prohibitive costs[3] and is unlikely to materialize.

22. In certain cases, it may be possible for the governing entity of the distributed ledger to decide to make changes to the protocol that are not compatible with past blocks. This may also affect persistence of information.

Finality of transactions

23. Transactions using DLT are broadcasted and distributed to the network. Generally, finality is deemed to be achieved once the transaction is irreversible and a block has been added to the distributed ledger and it cannot be deleted. In certain DLT systems, this leads to situations where the finality of the transaction is achieved only when the network has agreed on accepting the block.[4] A transaction is then considered irrevocable, and finality of the distributed ledger is achieved.

Non-discretionary automated execution

24. Another feature of DLT is the reduced discretionary nature of the execution of commands contained in scripts stored in the distributed ledger (DLT-based automated contracts or "smart contracts"). Like other automated contracts, a DLT-based automated contract is self-executing when predefined conditions are met. Due to the inability of the parties to unilaterally amend the scripts, there is greater certainty that the instructions will be executed, thus improving the efficiency and predictability of operations. However, this feature of DLT may pose challenges when the law requires the inclusion of software that stops the execution of the automated clause ("*kill switch*").[5]

Pseudonymity

25. While pseudonymity may not necessarily be an obstacle to identification of the party, it may hinder that identification, particularly if the law requires the use of a certain method or procedure, or the fulfilment of a specific level of assurance of

[3] This is the cost to be in control of 51 per cent of the distributed ledger by purchasing the needed cryptocurrency at market capitalization rate.

[4] For instance, in the case of Bitcoin finality is achieved when approximately six further blocks are added to the digital ledger after the block containing the relevant transaction.

[5] See, e.g. 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, i.e. "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".

identity. If reliable identification is not possible, additional measures such as anomaly and fraud detection[6] may be needed, for instance to avoid insider trading of digital assets stored on the ledger.

26. 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 Model Law on Electronic Transferable Records ("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).

27. A specific issue may arise when serving legal notices to a pseudonymous address. In those jurisdictions where the law is more flexible on such matters, specific procedures have been devised for service of judicial documents, namely in cases relating to cryptocurrencies. For instance, courts have attempted to serve court documents via social media or by messaging the defendant's cryptocurrency wallet address. Courts have also allowed for the service of documents by *non-fungible tokens* ("NFTs") delivered in the wallet ("airdrop").[7] However, in some jurisdictions the use of such mechanisms for service of documents has been regarded as a violation of due process.[8]

Lack of interoperability

28. In general, DLT lacks cross-ledger interoperability, i.e. an individual distributed ledger is not designed to interact with another distributed ledger or with non-DLT applications. This is because distributed ledgers, especially those private and custom-built, are designed with a specific focus (or focuses) in mind and do not operate beyond their boundaries. Lack of interoperability may limit the applications of distributed ledgers and their benefits as information remains in a "*data silo*" and cannot be easily transmitted to or used in other systems. Technical work has started to overcome this technical limitation[9] and to ensure standardization that will facilitate interoperability.[10]

D. The law applicable to DLT

Principles underlying UNCITRAL e-commerce texts

Technology neutrality

29. 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 if technology advances, further legislative work is not required as technology neutral rules already accommodate any future development. Thanks to technology neutrality, UNCITRAL texts are generally supportive of the use of DLT.

30. The definition of "electronic record" contained in article 2 MLETR has been expanded to encompass "all information logically associated with or otherwise linked together so as to become part of the record, whether generated contemporaneously or not" to confirm its application to DLT-based applications. That definition is closely

[6] Anomaly and fraud detection mechanisms include analysing data (either statistically or using machine learning) to detect any anomalies in activities and patterns.

[7] 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).

[8] X v Y, Gerechtshof Amsterdam, 29 January 2019, ECLI:NL:GHAMS:2019:192, CLOUT Case 1921.

[9] See, e.g. the Cross-chain by Chainlink protocol, and the Polkadot Network ecosystem.

[10] E.g. see the work programme of the ISO/TC307 technical committee on Blockchain and distributed ledger technologies.

related to the definition of "data message", which ensures the technological neutrality of UNCITRAL texts on electronic commerce.

Legal recognition

31. Provisions contained in UNCITRAL texts give legal recognition to the use of electronic means (and prohibit discrimination against that use) on a technology-neutral basis. Those provisions therefore also apply to the use of DLT.

32. Conversely, as DLT is based on the use of encryption technologies, jurisdictions that have adopted laws restricting the use of those technologies (e.g. by recognizing legal effect only to electronic signatures issued in compliance with national encryption standards and schemes) may limit the ability to give legal recognition to the use of DLTs. Moreover, such legislative choice may be incompatible with provisions in trade agreements that mandate the use of technology-neutral electronic signature or electronic authentication methods.

Functional equivalence

33. The principle of functional equivalence enables the satisfaction of paper-based form requirements with the use of electronic means. Besides fulfilling certain conditions, functional equivalence presupposes the use of reliable methods to achieve the intended purpose. Features of DLT such as persistence of information and assurance of singularity may facilitate satisfying certain functional equivalence requirements contained in UNCITRAL texts.

34. As noted (Taxonomy, para. 200), the technologies and methods supported by a DLT system to implement the distributed ledger render the data recorded therein "immutable" in the sense of remaining complete and unaltered from the time it was first entered in the ledger. Those qualities correspond to the concept of "integrity" under UNCITRAL electronic commerce texts, which is relevant for certain functional equivalence rules:

(a) Article 8 of the UNCITRAL Model Law on Electronic Commerce ("MLEC") prescribes integrity as one of the functions that a data message containing information 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 which arises in the normal course of communication, storage and display. The same requirement is contained in article 9(4) of the United Nations Convention on the Use of Electronic Communications in International Contracts ("ECC"). Methods that use DLT may provide a higher level of reliability with regard to assurance of integrity;

(b) Under article 10 MLETR, integrity is one of the functions that an electronic transferable record must fulfil in order to be legally equivalent to a paper-based transferable document or instrument;

(c) Article 6(3)(d) of the UNCITRAL Model Law on Electronic Signatures ("MLES") 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 also in DLT systems. In a similar vein, article 17 MLIT prescribes integrity as one of the functions of electronic seals.

35. Similarly, persistence of information may assist in satisfying requirements contained in UNCITRAL texts relevant for evidentiary purposes. For instance:

(a) Article 9 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;

(b) Article 19 MLIT, on electronic archiving services, requires that the archived data message be retained in the format in which it was generated, sent or

received, or in another format which 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.

36. In this regard, under European Union ("EU") law[11] the use of a trust service named "electronic ledger" is associated with a presumption of the unique and accurate sequential chronological ordering and of the integrity of data records contained therein when certain additional conditions are met ("qualified electronic ledger"). In the same law, "electronic ledger" is defined as "a sequence of electronic data records, ensuring the integrity of those records and the accuracy of the chronological ordering of those records".[12]

37. Singularity is the assurance that the digital object (e.g. a commercial document in electronic form) exists only in a single electronic record. NFTs are a specific application of DLT that may offer a higher level of assurance of singularity of a digital object because of their technical specifications. Thus, for instance, NFTs may facilitate fulfilment of the singularity requirement of electronic transferable records set in article 10(1)(b)(i) MLETR.

Use of DLT in electronic contracting

Location of equipment

38. DLT having a decentralized nature, its various parts may be located in different jurisdictions, or may also change regularly location. For this reason, rules indicating that the location of equipment and technology supporting the information system is not necessarily the place of business of a party (article 6(4) ECC) may be useful when DLT is used. The definition of "information system" as "a system for generating, receiving, storing or otherwise processing data messages" (article 2(f) MLEC and article 4(f) ECC) encompasses distributed ledgers.

Automated execution

39. As noted (para. 24 above), the use of DLT may increase the confidence in the automated execution of contracts by reducing the possibility of their unilateral modification. The DLT-based automated contract may be set to execute automatically when certain parameters are fulfilled. Metadata and data generated from off-ledger objects such as oracles may also be used as a condition for triggering the automated execution of contracts.[13]

40. From a practical perspective, it should be noted that executing contractual terms in an automated manner may be challenging where clauses that require consideration of specific facts and circumstances, such as force majeure and compensation clauses, are concerned. Arguably, it may be possible to identify and clarify those facts and circumstances to allow automated execution. However, considering the number of conditions to be clarified and the complexity of the scenarios, from a practical standpoint contractual parties may prefer not to automate such clauses.

Electronic signatures

41. From a technical perspective, cryptography lies at the core of DLT. Electronic signatures based on cryptography are used in distributed ledgers to authenticate and authorize operations executed through automated contracts.

---

[11] Article 45k of the 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"), as amended by Regulation (EU) 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 ("eIDAS 2 Regulation").

[12] Article 3, point 52 of the eIDAS Regulation, as amended.

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

42. From a legal perspective, DLT-based electronic signatures may be used to identify the signatory and to express its intent with regard to the signed message, thus fulfilling the conditions 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 that use DLT, which could therefore be legally recognized.

43. On the other hand, the law may require the use of specific technologies or services (such as "qualified signatures" or "digital signatures") and may impose the use of national technical standards and providers (see para. 32 above). DLT-based electronic signatures may not meet those additional requirements, for instance because their decentralized nature does not permit localization of the distributed ledger system in one jurisdiction only.

44. A peculiar application of electronic signatures in the DLT environment pertains to the use of *multi-signature ("multisig") wallets*, in particular to approve transactions on digital assets. In this case, multiple PKI-based signatures from predetermined addresses are required to proceed with the transaction. More generally, this technology may be used when multiple signatures from different parties are required to authorize a transaction (e.g. in public procurement, for escrow accounts, etc.).

DLT and PIL

45. PIL challenges 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.

46. In general, PIL rules assist in determining the applicable law. However, actors of a DLT system at the infrastructure layer (see para. 47 below) can be scattered across multiple jurisdictions, and the distributed ledger itself may be located in multiple jurisdictions, or its location may vary constantly. For this reason, PIL rules that refer to territorial connecting factors may not be adequate in a DLT context.[14]

E. Issues relating to the infrastructure layer

47. The infrastructure layer of DLT systems refers to the network and the distributed ledger that uses it. Relevant components are hardware, data, consensus, and programming. The actors involved are the developer, i.e. a person or group of persons who designs, develops and maintains the computer code that runs the system, and the node operator (Taxonomy, para. 176). In short, the infrastructure layer provides the DLT to the enterprise.

Responsibility for business continuity management and service standards

48. *Business continuity management* ("BCM") is the process of ensuring that an organization can continue to operate in the event 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. *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 levels, and taking corrective action when necessary to ensure that service levels are being met.

49. Business continuity and good service level management are crucial in building confidence in the use of distributed ledgers. For enterprises that wish to use DLT systems in their business operations, the choice of developing in-house DLT systems

[14] See HCCH Prel. Doc. No 4 of November 2020, Annex I, for a list of PIL connecting factors and their use in a DLT context.

or outsourcing them to a third-party developer depends on the scale of the business operations. An enterprise with enough scale may develop its in-house DLT system. If the enterprise intends to operate the DLT system and to offer it for use or access to third parties, the enterprise may become responsible for maintaining a certain level of service as a developer, operator, or both.

50. When outsourcing DLT systems, enterprises should ensure that the developer has BCM plans and that a minimum level of service is met. Due diligence is recommended when assessing such issues, which may take place during counterparty vetting but also during service provision. Possible measures include a request of the track record of the developer, request for 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.

51. Enterprises may consider contracting with developers to set out BCM plans and the expected minimum standard of service. In addition, enterprises may consider enacting in-house guidelines or policies on minimum standards that third-party service providers must meet before contracting with them. Amendments to existing BCM clauses may be required to tailor them to the features of DLT. Due diligence, coupled with a contract that clearly sets out the rights and obligations of the parties, can reduce the chances of non-performance of the DLT service provider.

Audit procedures and the right to audit

52. One issue relevant for the relationship between the distributed ledger service provider and user is the right to audit and the enforcement of auditing procedures. 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 sieve out dysfunctional or fraudulent codes and identify any potential vulnerabilities or weaknesses in the DLT system.

53. In cases where enterprises outsource the development of the distributed ledger or its operation, enterprises may consider inserting in the contract with the developer and the operator a clause that grants them the right to audit the code. This gives enterprises the contractual right to conduct their own audits of the third-party developer's code. As most of this code would be implemented in the enterprises' own servers or information technology systems, the right to audit and an agreement on how such audit should be conducted are important mechanisms to protect enterprises against cybersecurity attacks exploiting errors in the code.

Environmental concerns

54. In the Proof of Work consensus mechanism, which forms the basis of cryptocurrencies such as Bitcoin, high energy consumption is required to verify that transactions have been executed on the distributed ledger. Regulators are concerned about the environmental footprint for distributed ledger *mining*.[15] Reducing electric consumption caused by the Proof of Work mechanism is desirable, and several initiatives aim to decarbonize the cryptocurrency industry.[16] The move from the Proof of Work to the Proof of Stake consensus mechanism may reduce energy costs in relation to cryptocurrency mining.[17]

55. Considering the high amount of electricity consumed by distributed ledger mining, regulation or reporting requirements on such activities may become more

[15] For more information 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, https://inweh.unu.edu/.

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

[17] The Ethereum network moved from the Proof of Work mechanism to the Proof of Stake mechanism, which significantly decreased energy usage and carbon footprint.

common and comprehensive in the future. Enterprises that engage in distributed ledger mining should be aware of legislation that may regulate such activities.[18]

F. Issues relating to the application layer

56. The application layer is where DLT is used to offer products and services. The actors involved are the enterprise offering the products and services and the users of the products and services.

Contract automation

57. DLT-based automated contracting has been promoted as a major advantage of DLT systems due to the higher degree of confidence in the automated execution of the code (see para. 24 above). The UNCITRAL draft provisions on automated contracting (A/CN.9/1178 and A/CN.9/1179) provide guidance, on a technology-neutral basis, on legal issues that may arise when using contract automation. The draft provisions do not deal with the probability that the script will be executed, which is a business rather than a legal consideration. They also do not deal with considerations on how to automate certain contractual terms (see paras. 39–40 above).

Liability for incorrect information

58. An aspect of liability and risk allocation pertains to instances where the information on the distributed ledger is inaccurate, either due to a good faith mistake or fraudulent behaviour. This may happen at the development stage (e.g. inserting malicious code while deploying the distributed ledger) or during information input (e.g. information was entered that was known to be inaccurate) (see para. 20 above).

59. With respect to input of data, the liability for recording inaccurate or false information remains with the person providing the information, or on whose behalf the information was provided. From a business perspective, enterprises should carefully consider quality of data input and possible remedial measures, especially if they rely on the distributed ledger for critical operations. Enterprises permitting users, in particular third parties, to access or use their private permissioned distributed ledger should enter into a contractual relationship to limit their liability towards users.

Data privacy and protection

60. Numerous States have enacted data privacy and protection laws that apply also to DLT-based applications. For instance, the EU General Data Protection Regulation ("GDPR")[19] applies when personal data is involved, including when DLT is used. In that regard, it has been suggested that a public key may be considered personal data under the GDPR given the analogies between public keys and dynamic IP addresses.[20]

61. When implementing distributed ledgers, enterprises should consider whether personal data will be stored on the distributed ledger and should take active steps to comply with applicable data privacy and protection laws. As the developer, operator and user can be located across multiple jurisdictions, contractual clauses should be inserted in the services agreement to ensure compliance with all relevant data privacy and protection laws.

---

[18] For instance, the US Crypto-Asset Environmental Transparency Act of 2022 requires parties who consume more than five megawatts of power when undertaking crypto mining operations to report their carbon dioxide emissions under the Clean Air Act.

[19] 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.

[20] 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.

Storage of data ("right to be forgotten" and "right to deletion")

62. 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 data or information in question are highly sensitive personal data, such as healthcare records or biometric information. Moreover, the decentralized nature of DLT means that personal information of a person resident in one jurisdiction could be stored in a different jurisdiction, and that the place of storage may vary regularly.

63. Furthermore, because of the decentralized nature of DLT, it may be difficult to identify a data controller or other entity responsible for enforcing the "right to be forgotten" and the "right to deletion". This may be further complicated by possible challenges in identifying that entity due to pseudonymity.

64. The counterargument on a conceptual level is that the DLT is not always strictly immutable, and that developers and administrators can agree to remove certain data, at least from private permissioned ledgers. However, this solution does not address data deletion in public permissionless ledgers.

65. Another possible solution is the storage of personal data in a database that is not on the distributed ledger. Such solution does not however solve the problem of the right to delete, and it may increase costs.

66. Alternatively, DLT platforms may implement privacy-enhancing features that allow data to be encrypted or anonymized, so that it cannot be easily traced back to an individual. However, these measures may not always be sufficient 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, e.g. because of the use of a public permissionless ledger, data minimization in processing information across the network could be pursued (see para. 69 below).

Right to amend information stored incorrectly

67. Another operational issue with data persistence is that 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 like that of the right to be forgotten, i.e. setting up pre-defined governance rules and reducing centralization in favour of control over data.

68. Code has been released and published that allows the revision or deletion of data at the user's request. This technical solution provides enterprises with an additional possibility of complying with data privacy and protection law.

Mitigating measures

69. To mitigate the above-mentioned issues, enterprises may use privacy-enhancing features such as *Zero-Knowledge-Proofs* ("ZKP"). ZKP is a method by which one party (the "prover") can prove to another party (the "verifier") that a given statement is true while the prover avoids conveying any additional information apart from the fact that the statement is indeed true.

70. Enterprises may consider encrypting and anonymising 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 anonymisation will render access to the data useless.

Specific applications: digital assets

71. The legal treatment of data storing value, which is generally described as "digital assets", has attracted significant attention. While any data has some value, and therefore may fall within the definition of digital asset, the legal notion of "digital asset" often refers to storage and transfer of value with the use of DLT. States have

different approaches to the definition of "digital assets". For instance, the United States of America Commodities and Futures Trading Commission ("CFTC") appears to place emphasis on the control and transferability of the digital assets,[21] while the European Union appears to focus on what the asset "represents", i.e. the rights that the token incorporates.[22] The Taxonomy recognizes the lack of a 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).

72. Laws have been drafted with the aim of filling legal gaps in the regime applicable to digital assets.[23] Some of these laws safeguard the application of other laws, in particular, law applicable to commercial documents and to money. With regard to PIL, the HCCH PB is conducting a lex specialis study focusing on PIL questions raised by specific cross-border use cases of digital tokens.[24]

73. Due to the variety of applications regarding digital assets that involve the use of DLT, it is desirable to consider separately legal issues arising from different types of digital assets.

Payment services and cryptocurrencies

74. Digital assets may be used to transfer value.[25] These digital assets are often referred to as cryptocurrencies. Cryptocurrencies may have a market value, if sufficiently liquid to be traded in dedicated markets ("*crypto-exchanges*"). Some cryptocurrencies link their value to fiat money or other goods to mitigate volatility ("*stablecoins*").

75. Cryptocurrencies may be seen as a more stable and more effective form of value transfer where national currencies are highly volatile or restrictions on cross-border payments are in place. In some States, cryptocurrencies have been declared legal tender besides the national currency. This has however raised novel questions, for instance on the exchange rate between the pre-existing currency and the cryptocurrency and, more generally, on monetary policy.

76. Challenges arising from the use of cryptocurrencies are of legal, regulatory and business nature. The legal qualification of a cryptocurrency, including the applicable regulatory regime, depends on its features. Regulators are increasingly considering digital assets as commodities, securities, or both.[26] Payment services carried out using DLT systems are subject to payments law.

77. With regard to legal issues, a yet unsettled matter relates to the ability to classify cryptocurrencies as property. In those jurisdictions where this is possible, cryptocurrency holders may use proprietary remedies, e.g. the freezing of an asset.[27]

78. From a business perspective, cryptocurrencies, including stablecoins, may be highly volatile. If enterprises wish to use cryptocurrencies for payments, they may

[21] CFTC, Digital Asset Markets Subcommittee Recommendation – Adoption of an Approach for the Classification and Understanding of Digital Assets, 7 March 2024.

[22] Global Blockchain Business Council, Regulatory Map.

[23] In the United States, UCC Article 12; Unidroit Principles on Digital Assets and Private Law; Dubai International Financial Centre (DIFC) Digital Assets Law, Law No. 2 of 2024.

[24] HCCH C&D of March 2024, No 12.

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

[26] In some cases, cryptocurrencies may be qualified as commercial documents. For instance, a commoditized stablecoin (i.e. 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.

[27] 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/CN.9/WG.V/WP.192 and A/CN.9/WG.V/WP.193).

consider using different crypto-exchanges and cryptocurrencies to mitigate risks if the exchange or the currency proves to be problematic, including in case of sudden default of the crypto-exchange.

79. Central bank digital currencies ("CBDCs") are defined as fiat money issued in electronic form. As such, they are issued by central banks only and are different in nature from cryptocurrencies.[28] CBDCs pilot projects, which often involve the use of DLT,[29] have focused on the retail use of CBDCs.[30] The HCCH has established an Experts' Group on the applicable law and jurisdiction issues raised by the cross-border use and transfers of CBDCs.[31]

Electronic transferable records

80. In practice, electronic transferable records, as defined in the MLETR, may be issued using DLT-based applications. Those records are transferable documents and instruments in electronic form, and, as such, the substantive law of those documents and instruments applies together with the rules contained in the MLETR. The explanatory note to the MLETR provides specific guidance on selected DLT-related issues. For instance, the 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).

81. 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 a law that enables the use of both paper-based and electronic documents by adopting a medium-neutral approach. The draft UNCITRAL–UNIDROIT model law on warehouse receipts (A/CN.9/1182) provides an example of the latter approach.

G. Issues relating to the governance layer

82. Due to the decentralized nature of DLTs, special governance issues may arise in relation to the infrastructure layer, particularly in the case of public permissionless distributed ledgers. These governance issues arise due to the lack of a central authority, as decisions are normally made via voting based on governance tokens. The holders of those tokens may not be aware of each other's existence or may even not be identified as they operate under a pseudonym. This is the governance layer.

83. Litigation against the subjects involved in the governance layer is not uncommon. While such litigation may generally involve any issue arising from the malfunctioning of the distributed ledger system, in practice litigated cases often relate to loss of digital assets due to hackers exploiting programming errors. As it is often impossible to pursue justice against the hackers for practical reasons, the aggrieved parties ask compensation from the subjects involved in the governance layer and allegedly responsible for the programming errors.

---

[28] The International Monetary Fund has released a CBDC 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 CBDC Virtual Handbook is available at www.imf.org/en/Topics/fintech/central-bank-digital-currency/virtual-handbook.

[29] E.g. Project mBridge uses a dedicated distributed ledger for multi-CBDC cross-border payments; see www.bis.org/about/bisih/topics/cbdc/mcbdc_bridge.htm.

[30] 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.

[31] HCCH C&D of March 2024, Nos. 9 and 10.

84. From a broad perspective, the ability to bring claims against node operators, developers or decentralized autonomous organizations' ("DAO") members (see para. 98 below) depends on the type of distributed ledger and its purposes. A breakdown of roles may assist in examining liability profiles. Generally, there are four key roles relevant for discussing liability and DLT: the developers of the code, the operators of the DLT, the users of the DLT, and the parties who claim damage. Electronic signatures based on cryptography are used to establish roles linked with a pseudonym.

85. One of the key issues arising from the use of a decentralized governance structure is that it may be challenging to agree on rights and obligations of each party, especially when using public permissionless distributed ledgers, because of the uncertainty in acknowledging decentralized governance structures as legal entities. In many cases, even identifying the entities involved may be difficult due to the use of pseudonymity.

86. Counterparty risks may be reduced when engaging developers to build private permissioned distributed ledgers. Because of the clear identification of the counterparty, enterprises may conduct due diligence by ensuring that they are contracting with a legally recognized entity, verifying the company's track record of building and maintaining DLT systems, etc.

87. Enterprises that use private permissioned distributed ledgers for commercial purposes generally face less difficulties in case of claims against a developer because there is certainty on the identity of the developer and on the terms under which the code has been developed and deployed.

88. On the other hand, claims against developers of a public permissionless distributed ledger can be more complex. First, extensive work may be needed to identify developers or node operators who operate under a pseudonym. Second, it is debatable whether and what type of legal relationship is established (e.g. in the form of a fiduciary duty) to determine rights and obligations between the affected party and the developer or operator.[32] Third, enforcing judgments against the developers or node operators may be challenging due to geographic remoteness.

89. Furthermore, it may be challenging to ascertain the legal personality of the developer or operator (i.e. in the case of a DAO), thereby making it difficult to attribute liability to the parties involved. Enterprises may mitigate risks by purchasing insurance coverage, if such insurance is available and applicable to their business operations.

90. Litigation relating to developer liability in public permissionless distributed ledgers is seen in lawsuits against cryptocurrency developers. In one such case, a Bitcoin owner who lost assets due to a hack on his account sued the developers of Bitcoin to develop a software patch to restore access to the account based on a fiduciary duty between developers and users.[33] It has been found that a viable argument that the developers owe a fiduciary duty to users may exist.[34]

Decentralized Autonomous Organizations

91. DLT has inspired the creation of a specific entity known as DAO to govern them. DAOs are a DLT-based governance structure that can be used by any profit or

[32] To remedy this gap, https://jonasgross.medium.com/legal-aspects-of-blockchain-technology-liability-8f5b433030fit has been suggested to bring claims under product liability law in those jurisdictions where such claims are not limited to physical injury but include financial losses. In those cases, product liability in the DLT context is normally sought against the developers but rarely against the operators.

[33] Tulip Trading v Bitcoin Association, 25 March 2022, [2022] EWHC 667 (Ch).

[34] The decision by Falk J in Tulip Trading v Bitcoin Association was appealed by the claimant and allowed on appeal. The case will proceed trial to find if the fiduciary duty exists in the specific case: see the appeals judgment by Lord Justice Lewison, Lord Justice Popplewell and Lord Justice Birss, Tulip Trading v Van der Laan, 3 February 2023, [2023] EWCA Civ 83.

non-profit organization. Several governments and institutions have defined DAOs; for instance, the European Central Bank has defined DAOs as “virtual organisations built and run on code and blockchain technology”. Other institutions have provided more detailed definitions: e.g. the United States Department of the Treasury defines DAOs as “a system of administration that operates according to a set of encoded and transparent rules or smart contracts”.

92. Common key elements of DAOs may be identified. DAOs operate using DLT-based automated contracts. They are normally decentralized with multiple members across various jurisdictions. As a result, the governance structure and legal status of a DAO is a prominent issue to establish a contractual relationship or to attribute liability among parties.

93. The variable form and decentralized nature of a DAO means that DAOs can take hybrid governance structures.[35] It is therefore important to describe the governance structure of DAOs in order to discuss legal issues arising from it. Inability to correctly attribute legal personality to a DAO has wide ranging consequences for enterprises that transact with DAOs and for the members of the DAOs, who may face personal liability for the DAO’s actions.

Governance structure of DAOs

94. DAOs may use different organizational structures. Decision-making may be restricted to the founders of the DAO, may be automated through software protocols, or the voting weight may be distributed based on the type and number of tokens controlled. DAOs use DLT-based automated contracts to set out the rules on the purpose of the DAO, how members agree to cooperate, how decisions are collectively taken through a voting process, how native tokens are created and distributed, and how transactions are executed once certain conditions are met.

95. The governance structure of a DAO is driven by DLT-based automated contracts. Hence, DAOs require a structured decision-making process. In absence of a central authority, the consensus and dispute resolution mechanism are of outmost importance, e.g. by majority vote or by algorithms. The first step involves determining who may submit a proposal for a course of action. Then, a decision-making body or algorithm makes a decision.

96. Certain DAOs allow only members holding a specific digital asset (so called “governance token”) to participate in the decision-making processes. Oftentimes the weight of a vote is proportional to the amount of the specific digital asset held in custody. The specific digital assets are often obtained by investing into the DAO or by allocating work time to the DAO or by supporting the DAO in other ways (e.g. as marketing ambassador).

97. Compared to traditional corporate mechanisms where decisions are made by board of directors or chief executive officers, decisions by DAOs usually depend on group consensus or member voting. DAOs are generally free to define their governance structure to meet the objectives of the organisation, making it a flexible tool for a broad range of collaborative purposes. However, preliminary empirical evidence shows that governance tokens are disproportionately allocated to founders and core developers.

98. Usually, DAO governance is based on rules or codes of conduct, which are public and available through white papers, websites or applications. However, these rules do not have the same legal binding force as traditional corporate organizational tools.

[35] Hybrid governance structures allow for a certain degree of centralization that also incorporates elements of decentralization. From a commercial perspective, this can entail allowing users to weigh in on certain decisions that the enterprise may make, e.g. future product designs and updates.

99. In some DAOs, members of the DAO use pseudonyms. The general principles on pseudonymity and party identification apply to DAOs as well.

100. The typical features of a DAO, some of which may pose risks for enterprises, are:

(a) Decision-making: rules for consensus are typically defined at an early stage and are relatively difficult to amend over time when the DAO grows in size and complexity, which may lead to an inadequate consensus mechanism, e.g. slow and inefficient. This may ultimately limit the DAO's operation or even impede a prompt reaction to unforeseen situations;

(b) Lack of accountability: decisions in a DAO often involve many parties, therefore diffusing responsibility, a notion known in social psychology that leads individuals to feel less responsible. As a result, due to reduced accountability DAO without central oversight may be prone to mismanagement of resources;

(c) Lack of representation: depending on the system of representation implemented, e.g. with voting rights proportional to the holding of a specific digital asset, some DAO members may feel underrepresented in the decision-making process, potentially leading to reduced acceptance of the decisions, dissatisfaction, and conflicts;

(d) Security vulnerabilities: DAOs rely on DLT-based automated contracts that are relatively difficult to amend in the case of an identified security vulnerability. This potentially leaves the DAO exposed to cyberthreats or fundamental challenges such as in case of a faulty voting or payout mechanism.

101. Enterprises that decide to engage in commercial transactions with a DAO should be aware of these risks. Steps that may limit risks when working with a DAO include verifying the incorporation status of the DAO and requiring the DAO to identify its members and developers so that the enterprise can proceed on the basis of personal liability in a worst-case scenario.

Contractual obligations and liability issues applicable to DAOs

102. DAOs may be appealing to enterprises due to their potential for transparency and customization. However, there are also potential issues: DAOs raise significant legal uncertainty due to their undefined organization structure. Due to the range of possible types and structures of DAOs, each DAO must be evaluated on a case-by-case basis to determine which law applies.

103. Absent specific legislation, attempts were made to categorize DAOs into a type of existing legal entity, such as a general partnership, a limited liability partnership, or a non-profit organization.

104. Some States have introduced specific legal mechanisms (sometimes called "legal wrappers") to provide DAOs with a legal personality, for instance by permitting their registration.[36] These laws normally provide protection of a legal entity and allow DAOs to limit their liability like a limited liability company.[37] This simplifies dealing with DAOs by significantly increasing legal predictability.

105. In States where DAOs can be incorporated but have failed to do so, regulators have sought to pin down liability on individual members and making them personally

[36] In the United States, e.g. Tennessee, Tennessee Code Annotated, Title 48, as amended; Vermont, Blockchain-Based Limited Liability Companies, 11 V.S.A. § 4173, and Wyoming: Wyoming Decentralized Unincorporated Nonprofit Association Act, Wyoming Statutes, Title 17, Chapter 32. See also the Decentralized Autonomous Organization Act, 2022, of the Republic of the Marshall Islands.

[37] For instance, Vermont allows for the registration of a "blockchain-based limited liability company" ("BBLLC"), which requires the blockchain-based limited liability company to specify "whether the decentralized consensus ledger or database utilized or enabled by the BBLLC will be fully decentralized or partially decentralized and whether such ledger or database will be fully or partially public or private" (Vermont Statutes Annotated, Chapter 11, § 4173).

liable.[38] The legal consequence is usually the unlimited personal liability of the "partners" (i.e. the token holders) of the DAO.

106. 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 pseudonymous and do not reside in the same State.

107. The legal qualification of a DAO determines the applicable insolvency regime. However, some peculiar insolvency-related questions may arise from the nature of the DAO and the use of DLT. For instance, members of the DAO may be seen as creditors or, alternatively, as debtors of the insolvent DAO; governance tokens may be considered as property; members and directors, if any, may be seen as owing fiduciary duties to each other and to users, etc.

The COALA Model Law

108. Several academic institutions have conducted projects to resolve legal issues surrounding DAOs. The Coalition of Automated Legal Applications ("COALA") is a think tank which explores legal issues arising from the decentralized economy and distributed ledger technologies. It has released a COALA Model Law for Decentralized Autonomous Organizations ("COALA Model Law") that provides rules on the governance and operation of DAOs.[39]

109. The COALA Model Law adapts the concept of functional equivalence to the context of DAO. It suggests that establishing functional equivalence is "useful for simplifying the regulation of DAOs" and that this requires "to identify a policy objective or a purpose and then demonstrate that this objective or purpose could be achieved either by the enforcement of a legal rule or by relying on a particular application of technology".[40] One example provided by the COALA Model Law on functional equivalence is as follows:

> "For example, instead of introducing new corporate rules specifically applicable to 'tokenized' shares, shares that are recorded on a blockchain-based system could be regarded as valid titles to a share, transferable via a blockchain-based registry. Regulatory equivalence relies on the same technique but identifies the object or purpose of any given regulation as goal. It allows for the establishment of equivalence between the function of a legal rule and the function of a technology."[41]

110. Under the COALA Model Law, the issue of legal personality is resolved by explicitly providing DAOs with a legal personality separate and distinct from its members (article 2 of the COALA Model Law).

[38] Commodity Futures Trading Commission v Ooki DAO, United States District Court Northern District of California, Case No. 3:22-cv-05416-WHO. The court held that "the Ooki DAO is a 'person' under the Commodity Exchange Act and thus can be held liable for violations of the law". The court then held that the Ooki DAO did, in fact, violate the law as alleged.

[39] In the United States, the Utah Decentralized Autonomous Organizations Act, Utah Code, Title 48, Chapter 5, is based on the COALA Model Law.

[40] COALA, Model Law for Decentralised Autonomous Organisations, p. 8.

[41] Ibid., p.3.

III. Glossary

Business continuity management: the process of ensuring that an organization can continue to operate in the event 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 sized. This output can be stored and later used for verification purposes.

Crypto-exchange: a trading platform or market 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 sieve out dysfunctional or fraudulent codes or identify any potential vulnerabilities or weaknesses in the DLT system.

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

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

Mining hash rate: a unit of measurement of how much computational power is required for a miner to solve a given encryption puzzle.

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 whereby the asset is incapable of mutual substitution among individual units.

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

Pseudonymity: pseudonymity 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.

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 validated 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 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.

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, but with an additional requirement of ensuring third parties do not refer or link to such personal data that was provided by the organization or enterprise.

Service level management: this 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 levels, and taking corrective action when necessary to ensure that service levels are being met.

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

Zero-Knowledge-Proofs: a method by which one party can prove to another party that a given statement is true while the prover avoids conveying any additional information apart from the fact that the statement is indeed true.