United Nations A/CN.9/1116

General Assembly

Distr.: General
29 April 2022

Original: English

**United Nations Commission on International Trade Law**
**Fifty-fifth session**
New York, 27 June–15 July 2022

# Legal issues related to digital economy – advancing work on automated contracting and other progress

## Note by the Secretariat

Contents



V.22-02564 (E) 100522 110522

# I. About this note

1. This note reports on the progress made by the secretariat in its exploratory and preparatory work on legal issues related to the digital economy since the fifty-fourth session of the Commission[1] and invites the Commission to consider the next steps in the project:

(a) On the topic of automated contracting, this note synthesizes the conceptual discussion that Working Group IV held at its sixty-third session (4–8 April 2022) at the request of the Commission[2] and invites the Commission to refine the mandate of the Working Group, as appropriate (see chapter II below);

(b) On the development of a legal taxonomy of emerging technologies and their applications, this note provides the Commission with a preliminary draft of a newly completed section on the topic of distributed ledger systems (see annex) and puts forward a proposal for the Commission to mandate the secretariat to prepare a legal guide on issues relating to the operation of distributed ledger systems and the provision of services that leverage distributed ledger technology (DLT) (see chapter III below).

2. This note complements A/CN.9/1117, which presents a proposal for work on the topic of data transactions to be dealt with by Working Group IV in tandem with the topic of automated contracting, as identified at the fifty-fourth session of the Commission.[3] Background to the digital economy project is set out in the first progress report to the Commission (A/CN.9/1012, paras. 2–5).

# II. Advancing work on automated contracting

## A. Background

3. At its fifty-fourth session (2021), the Commission considered a proposal for legislative work on electronic transactions and the use of artificial intelligence (AI) and automation (A/CN.9/1065). Broad support was expressed to refer the issues identified in the proposal to Working Group IV, and the Commission mandated the Working Group to host a "focused conceptual discussion with a view to refining the scope and nature of the work to be conducted".[4]

4. That discussion took place at the sixty-third session of the Working Group (4–8 April 2022) on the basis of a note by the secretariat which outlined key concepts related to automated contracting, and developed the general contours of the proposed legal framework.[5] The discussion is reported in chapter V of A/CN.9/1093.

## B. Defining key concepts related to the topic

5. In its note, the secretariat explained "automated contracting" as the use of "automated systems" to negotiate, form and perform contracts (e.g. to generate or process data messages constituting an offer, the acceptance of an offer, the terms of a contract, or action taken in execution of the contract). In the Working Group, it was acknowledged that the definition of "automated messaging system" in article 4(g) of the United Nations Convention on the Use of Electronic Communications in International Contracts (ECC) – i.e. "a computer program or an electronic or other automated means used to initiate an action or respond to data messages or performances in whole or in part, without review or intervention by a natural person

[1] This is the third such progress report. The first progress report is contained in A/CN.9/1012. The second progress report is contained in A/CN.9/1065.
[2] *Official Records of the General Assembly, Seventy-sixth Session, Supplement No. 17* (A/76/17), paras. 25(e) and 236.
[3] Ibid., para. 237.
[4] Ibid., paras. 25(e) and 236.
[5] A/CN.9/WG.IV/WP.173.

each time an action is initiated or a response is generated by the system" – remained apt to describe the systems that were being used for automated contracting.

6. In its note, the secretariat reiterated the view that an "AI system" is a type of automated system with two distinguishing features that gives it the semblance of greater complexity and capability, "intelligence" and "autonomy". Those two features are (i) the use of "machine learning" techniques and (ii) the processing of large quantities of data from multiple sources. In the Working Group, it was similarly proposed to define AI systems by reference to the distinguishing features of AI systems that were legally significant, and not by reference to the techniques used. Broad support was expressed for the view that the defining feature of AI systems was their unpredictability, which stemmed from the use of "machine learning" techniques. There was general support for the view that the distinction between "deterministic" and "non-deterministic" operation (i.e. whether the system always generates the same output given the same input) provided an appropriate starting point for formulating a definition of AI system that captured the defining feature of unpredictability. A preference emerged for using the term "autonomous contracting" to clearly distinguish it from automated contracting.

## C. Mapping out a legal framework for automated (and autonomous) contracting

7. The Working Group discussed a range of issues related to the scope and nature of the topic.

8. First, there was broad support for compiling provisions of UNCITRAL texts relevant to automated contracting as a starting point. To that end, the following provisions of the 1996 UNCITRAL Model Law on Electronic Commerce (MLEC) and the ECC were identified:

(a) A provision on the legal recognition of data messages used in the formation of electronic contracts (ECC, article 8(1); MLEC, articles 5, 11(1) and 12);

(b) A provision on the legal recognition of contracts formed using automated systems (ECC, article 12);

(c) A provision on admissibility in evidence of data messages (MLEC, article 9);

(d) A provision on when and where a data message is dispatched and received (ECC, article 10; MLEC, article 15).

Conversely, it was suggested that a provision recognizing that data messages and electronic contracts can satisfy paper-based legal requirements as to form (ECC, article 9; MLEC, articles 6, 7 and 9) would not be relevant, indicating that the validity of automated contracts might need to be examined from an angle other than functional equivalence.

9. Second, it was suggested that work could review and update existing provisions that were relevant to automated contracting, guided by the principles of technology neutrality and non-discrimination against the use of electronic means. Several suggestions to adapt or expand those provisions were already put forward in the Working Group, as outlined in A/CN.9/1093.

10. Third, it was suggested that new provisions addressing the following legal issues could be considered: (a) attribution; (b) matters relating to state of mind; (c) precontractual disclosure of information; (d) traceability with respect to the operation of automated systems; (e) liability for the output of automated systems, particularly in event of data processing error; (f) non-performance or partial performance; (g) self-enforcement and automated dispute resolution; and (h) renegotiation.

11. Fourth, it was indicated that the defining feature of autonomous systems – i.e. unpredictability – might warrant the differentiated treatment of those systems in the

application of existing provisions and in the development of new provisions. Several suggestions were already put forward in the Working Group, including a condition that a reliable method be used by the system for the purposes of legal recognition, disclosure of information regarding the use and operation of the system, and a special liability regime on account of difficulties in tracing the operation of the system.

12. Finally, it was indicated in the Working Group that work should proceed on the basis of a review of business practice and use cases. It was also indicated that work could proceed incrementally – a first stage would involve compiling and revising existing provisions as applicable to automated contracting, while a second stage would involve developing new provisions on a broader range of issues.

### D. Next steps

13. The Commission may wish to consider the report of the discussion within the Working Group and the above synthesis with a view to refining the mandate of the Working Group in terms of the scope and nature of its work on the topic. Specifically, the Commission may wish to mandate the Working Group to proceed incrementally as outlined above (para. 12), and thus to request the Working Group, as a first stage, (a) to build on a compilation of relevant existing provisions of UNCITRAL texts that apply to automated contracting, to be prepared by the secretariat, (b) to revise those provisions, as appropriate, and (c) to identify new provisions, to be developed as a second stage, that address a broader range of issues, including those identified by the Working Group at its sixty-third session.

## III. Developing a legal taxonomy of emerging technologies and their applications

### A. Background

14. The legal taxonomy of emerging technologies and their applications has been developed incrementally by the secretariat to address topics identified within the Commission or reported to the Commission by the secretariat. The taxonomy serves as a record of the secretariat's exploratory work on legal issues related to the digital economy and as a map to guide future work (e.g. by informing the formulation and consideration of proposals for future work). Preliminary drafts of sections of the taxonomy on AI and automation,[6] data transactions[7] and digital assets[8] were presented to the Commission at its fifty-third session, while a preliminary draft of a section on online platforms,[9] as well as revisions to the sections on AI[10] and data transactions,[11] were presented at the fifty-fourth session. These sections have sought to analyse each topic from an international commercial law perspective by (a) defining the topic in legal terms, and (b) identifying the actors, legal relationships and legal issues involved in the deployment and use of associated technologies and applications.

15. At the fifty-fourth session, the Commission was informed that the secretariat planned to prepare a new section of the taxonomy on distributed ledger (including blockchain) systems, and that the taxonomy could serve as a basis for other activities of the secretariat in supporting the central and coordinating role of UNCITRAL within the United Nations system in addressing legal issues related to the digital economy and digital trade. In response, the Commission requested the secretariat to continue

[6] A/CN.9/1012/Add.1.
[7] A/CN.9/1012/Add.2.
[8] A/CN.9/1012/Add.3.
[9] A/CN.9/1064/Add.3.
[10] A/CN.9/1064/Add.1.
[11] A/CN.9/1064/Add.2.

to develop the legal taxonomy and authorized it to publish the content of the taxonomy.[12]

## B. Intersessional work

16. Since the fifty-fourth session of the Commission, the secretariat has further revised the section on data transactions to record its further work in preparing the proposal contained in A/CN.9/1117. The secretariat has also completed the section on distributed ledger (including blockchain) systems, as identified at the fifty-fourth session. A preliminary draft of that section is contained in the annex to this note. The secretariat will continue to coordinate with Unidroit with a view to revising the preliminary draft of the digital assets section. The secretariat is consolidating the various sections of the taxonomy with a view to publishing its content as a "living document".

## C. Proposal for future work on a legal guide on the use of distributed ledger (including blockchain) systems

17. As foreshadowed at the fifty-fourth session of the Commission, the preparation of the new section of the taxonomy on distributed ledger systems has identified areas for possible future work by UNCITRAL on legal issues arising from the use of distributed ledger (including blockchain) systems. Specifically, the exploratory work by the secretariat has revealed the need for legal guidance on the operation of distributed ledger systems (described in the taxonomy as the "infrastructure layer", see para. 13 of the annex) and on contracting for the provision of DLT-enabled services (described in the taxonomy as the "application layer", see para. 13 of the annex).[13] With regard to the latter, a review of standard contract terms for DLT-enabled services, particularly terms relating to service levels and limitations of liability, as well as commentary regarding use cases for distributed ledger systems in trade, suggests that raising awareness of the main legal issues could promote greater security and sustainability in digital transformation efforts. A publication by the secretariat in this space could also promote engagement of governing bodies within the United Nations system with UNCITRAL on legal issues relating to blockchain, which face similar legal questions when contracting for DLT-enabled services (see JIU/REP/2020/7, Recommendation No. 6).

18. The Commission is therefore invited to consider mandating the secretariat to prepare a legal guide along the following lines:

(a) The legal guide would be presented in a format similar to the *Notes on the Main Issues of Cloud Computing Contracts*[14] and would signpost other UNCITRAL texts and ongoing work that are relevant to the use of DLT, particularly in the areas of electronic transactions, identity management and trust services, data transactions, and automated contracting (particularly noting that the latter work is expected to cover issues related to so-called "smart contracts" deployed in distributed ledger systems: see A/CN.9/1065, para. 9);

(b) Work on the guide would focus primarily on contracting for DLT-enabled services and would thus use the summary of legal issues contained in paragraphs 32 to 34 of the annex as a starting point. The legal guide would provide explanations and guidance that are meaningful and useful to commercial operators, especially MSMEs and operators located in developing countries, in assessing whether DLT-enabled

[12] *Official Records of the General Assembly, Seventy-sixth Session, Supplement No. 17* (A/76/17), para. 227.

[13] The need for additional legal guidance is evidenced by a focus on legal and regulatory compliance in dedicated toolkits, e.g., World Economic Forum, "Redesigning Trust: Blockchain Deployment Toolkit", April 2021.

[14] The *Notes on the Main Issues of Cloud Computing Contracts* are available at https://uncitral.un.org/cloud.

services address their needs, and whether the use of such services will have a negative impact on their business. In short, the legal guidance would make commercial operators aware of the risks and opportunities related to the use of DLT;

(c) Consistent with existing UNCITRAL texts on electronic commerce, the proposed guidance would be sensitive to the principles of technology neutrality and non-discrimination against the use of electronic means, as well as the principle of party autonomy. Accordingly, it is not envisaged that the guide would take a position on whether particular trade-related activities should be enabled by DLT systems (as opposed to other technologies or methods), or that it would mandate specific rules to govern the provision of DLT-enabled services or the relations between the parties. It would instead build on the taxonomy in identifying how existing UNCITRAL texts on electronic commerce apply to the use of DLT, in a similar fashion as is suggested in paragraph 13 above with respect to automated contracting. For instance, the guide would complement the Explanatory Note to the UNCITRAL Model Law on Electronic Transferable Records, which addresses issues relating to the implementation of the model law through the use of distributed ledger systems that enable the issuance and use of electronic transferable records.

19. In preparing the legal guide, the secretariat would continue to coordinate with other international initiatives, including work being undertaken at Unidroit, particularly given the connection between distributed ledger systems and the digital assets that they support, and at the Hague Conference on Private International Law, whose Permanent Bureau is exploring the private international law implications of the digital economy, including with respect to distributed ledger systems.

# Annex

## Legal taxonomy of emerging technologies and their applications: distributed ledger systems (preliminary draft)

[*See paras. 14 and 15 of the cover note*]

## A. Relevance to international trade

1. Originating in the "blockchain" that was conceived to support an electronic cash system for online payments, systems supported by distributed ledger technology (DLT) are being used and proposed to support a variety of trade-related activities. As the United Nations Conference on Trade and Development (UNCTAD) has observed, prominent use cases for DLT-enabled applications are in the areas of online payments, finance, international trade, and global value chains.[1] It adds that, according to some estimates, the market for DLT-enabled applications is expected to reach over $60 billion in 2024, while one forecast quoted by the World Trade Organization in its 2018 *World Trade Report* expects the business value of distributed ledger systems to grow to over $3 trillion by 2030, representing a "global large-scale economic value-add".[2] For some observers, services enabled by distributed ledger systems herald new ways of trading and new items of trade, while the infrastructure supporting them present new opportunities for investment and collaboration. As the World Economic Forum puts it with respect to supply chains, "blockchain has the potential to revolutionize how companies compete and stakeholders collaborate".[3]

## B. What are distributed ledger systems?

### 1. Domestic and international definitions

2. The Bitcoin white paper referred to the original distributed ledger system (the "blockchain") as a network of computers constituting a "peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions".[4] Transactions were to be recorded in blocks forming a chain; no reference was made to a "ledger".

3. More recently, the International Telecommunication Union (ITU) has published a technical specification[5] which defines "distributed ledger technology" in terms of the technologies and methods that implement a record of data (the "ledger") that is retained on multiple networked computers (the "nodes"). Those technologies and methods include cryptographic techniques (like those used to support certain types of electronic signatures) and consensus mechanisms that are designed to ensure that the same data is retained on each node (i.e. "shared, replicated and synchronized") and that the data retained on each node remains complete and unaltered (i.e. "immutable"). A similar definition has been formulated by the International Organization for Standardization (ISO), according to which "DLT" is the technology that enables the operation and use of a distributed ledger that is "shared across a set of DLT nodes and synchronized between the DLT nodes using a consensus

[1] UNCTAD, *Harnessing Blockchain for Sustainable Development: Prospects and Challenges* (Geneva, 2021), p. 5. For specific use cases, see Deepesh Patel and Emmanuella Ganne, "Blockchain & DLT in Trade: Where Do We Stand?", November 2020.

[2] WTO, World Trade Report 2018, p. 35, citing Rajesh Kandaswamy and David Furlonger, "Blockchain-Based Transformation: A Gartner Trend Insights Report", 27 March 2018.

[3] World Economic Forum, "Redesigning Trust: Blockchain Deployment Toolkit", April 2021, p. 14. For specific use cases, see Deepesh Patel and Emmanuella Ganne, "Blockchain & DLT in Trade: Where Do We Stand?", November 2020.

[4] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", 31 October 2008, p. 1.

[5] ITU, *Distributed Ledger Technology Terms and Definitions*, Technical Specification FG DLT D1.1, 1 August 2019.

mechanism".[6] A "DLT system" is in turn defined as a system that implements a distributed ledger.

4. Distributed ledgers are maintained by computer code (i.e. software or "protocol") that is run on the nodes. The code determines the operations that each node performs with respect to the ledger, such as reading the ledger, submitting a new data entry to the consensus mechanism for recording in the ledger, and participating in the consensus mechanism. Both the ITU specification and the ISO standard acknowledge that some nodes may retain only a "partial replica" of the ledger.

5. At a national level, laws enacted in some jurisdictions with the aim of promoting, recognizing or regulating the use of DLT systems, as well as attracting investment in high-tech industries, have focused on describing the technologies and methods deployed to implement and maintain a distributed ledger. For example:

(a) In Belarus, Presidential Decree No. 8 of 2017 on the development of the digital economy employs the term "transaction block ledger", which it defines to mean "a sequence of blocks with information about operations performed in such a system built on the basis of given algorithms in a distributed decentralized information system using cryptographic methods of information protection";[7]

(b) In Italy, Law Decree No 135/2018,[8] which gives the same legal effect to documents recorded using DLT as an electronic timestamp, defines "DLT" to mean "technologies and IT protocols using a shared, distributed, replicable and simultaneously accessible ledger, decentralized and encrypted, which enable the registration, validation, updating and storage of data, whether encrypted or not, which cannot be modified or forged";

(c) In Malta, the Malta Digital Innovation Authority Act, 2018, defines "distributed ledger technology" – an "innovative technology arrangement" within the remit of the Digital Innovation Authority – to mean "a database system in which information is recorded, consensually shared, and synchronized across a network of multiple nodes, or any variations thereof". The term "node" is in turn defined to mean "a device and data point on a computer network";

(d) In the US state of Arizona, the Electronic Transactions Act was amended in 2017 to give legal recognition to certain uses of "blockchain technology", which it defines to mean "distributed ledger technology that uses a distributed, decentralized, shared and replicated ledger, which may be public or private, permissioned or permissionless, or driven by tokenized crypto economics or tokenless". The definition goes on to specify that "data on the ledger is protected with cryptography, is immutable and auditable and provides an uncensored truth".[9] A similar "blockchain enabling" law in the United States of America state of Vermont defines "blockchain" to mean "a cryptographically secured, chronological, and decentralized consensus ledger or consensus database maintained via Internet, peer-to-peer network, or other interaction",[10] while the Blockchain Technology Act in the state of Illinois defines "blockchain" to mean "an electronic record created by the use of a decentralized method by multiple parties to verify and store a digital record of transactions which is secured by the use of a cryptographic hash of previous transaction information".[11]

6. By referring to DLT systems as "decentralized", "accessible", "permissioned", "permissionless", "public" and "private", the definitions listed above signal the importance of the infrastructure and governance structures of DLT systems to

[6] ISO, *Blockchain and Distributed Ledger Technologies – Vocabulary*, ISO Standard No. 22739, 2020 ("ISO 22739:2020").

[7] Decree of the President of the Republic of Belarus No. 8 of 21 December 2017 on Development of Digital Economy, unofficial English translation available at http://law.by/document/?guid=3871&p0=Pd1700008e, clause 8 of Annex 1.

[8] Enacted with modifications by Law No. 12 of 11 February 2019.

[9] United States, *Arizona Revised Statutes*, title 44, chap. 26.

[10] United States, *Vermont Statutes*, title 12, sect. 1913.

[11] United States, *Illinois Compiled Statutes*, chap. 205, act 730, sect. 5.

understanding the legal issues that they engage, which are outlined later in this section. In other jurisdictions, definitions focus on the qualities of data recorded in the distributed ledger resulting from the application of those technologies and methods, without reference to infrastructure or governance structures. For example:

(a) In France, article L211-3 of the Monetary and Financial Code was inserted in 2017 by the so-called "Blockchain Law" to provide for securities entered in a "shared electronic recording device", which is in turn defined in terms of prescribed authentication requirements, which are that the device be operated in such a way as to ensure the integrity of entries;

(b) In Germany, the 2021 Electronic Securities Act ("eWpG") provides for the issuance of securities based on DLT systems ("cryptosecurities"). The eWpG defines a "cryptosecurity" as an electronic security that is recorded in a register that is tamper-proof, logs data in time sequence, and is protected against unauthorized deletion and subsequent modification;

(c) In Switzerland, the Federal Act on the Adaptation of Federal Law to Developments in Distributed Ledger Technology,[12] enacted in 2020, amends the Code of Obligations and Financial Market Infrastructure Act to introduce, among other things, a trading system for securities based on DLT systems. The legislation refers to "ledger-based securities" and securities held in "distributed electronic registers" without elaborating on the underlying technology or system. Rather, it defines "ledger" in terms of requirements of integrity (of data entries therein) and transparency (of data entries therein without third party intervention);

(d) In the European Union, a proposal to amend the eIDAS Regulation[13] to give legal recognition to "electronic registers" and to regulate the provision of trust services consisting of the recording of data into an "electronic register" defines the term "electronic ledger" as "a tamper proof electronic record of data, providing authenticity and integrity of the data it contains, accuracy of their date and time, and of their chronological ordering".[14]

### 2. Other ways of defining DLT systems

#### (a) Defining DLT systems in terms of trust

7. Owing to perceptions of the immutability and auditability of data recorded in the ledger, DLT systems are sometimes described in terms of "trust":

(a) In one sense, immutability and auditability mean that the ledger can be "trusted" and therefore that parties can transact in data recorded in the ledger – or enter into transactions that are recorded in that data – without recourse to a "trusted" third party bookkeeper;

(b) In another sense, immutability and auditability mean that the methods supported by the DLT system provide assurance as to the qualities of data recorded in the ledger, and therefore that the system itself provides a "trust service" with respect to that data (for more on the work of UNCITRAL on trust services, see paras. 37–40 below).

8. Immutability and auditability will likely be relevant in evaluating the use of DLT for a particular trade-related activity, which in turn may affect which parties are involved in those activities. However, "trust" is not a defining feature for the purposes of a legal analysis of DLT systems. Moreover, a legal analysis of DLT systems should avoid non-legal concepts such as immutability and auditability; while those features

[12] Law of 25 September 2020, *Federal Gazette*, 2020, p. 7801.

[13] 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.

[14] See European Commission, Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No. 910/2014 as regards establishing a framework for a European Digital Identity, document COM(2021) 281 final (3 June 2021).

are relevant to trade, they are ultimately a function of – and subject to – the code that runs a particular ledger and the governance structures of the particular DLT system. Similarly, technical concepts such as "consensus" (or "agreement") between nodes should not be confused with legal concepts or held out to represent the state of mind of the persons to whom the operation of those nodes may be attributable.

### (b) Defining DLT systems in terms of automation

9. DLT systems are sometimes described in terms of automation and real-time data exchange. This is particularly so for so-called "smart contracts" that are deployed in DLT systems and which automate transactions on the ledger, often in conjunction with data fed to or from points outside the system (i.e. "off-ledger") using a service or application commonly referred to as an "oracle". While automation and real-time data exchange are important features of trade digitalization, they are not a function of DLT. Instead, they represent technologies and services that can interface with a DLT system, just as they can interface with other information systems. A legal analysis of DLT systems should therefore avoid confusing DLT with the technologies and services that support automation and real-time data exchange. Legal issues related to so-called "smart contracts" and other uses of automation in contracting are addressed in the AI and automation section of the taxonomy (see A/CN.9/1012/Add.1).

### (c) Defining DLT systems in terms of platforms

10. DLT systems are sometimes described as "platforms". Applying the working definition of "online platform" elaborated in the online platform section of the taxonomy (see A/CN.9/1064/Add.3, para. 3), all DLT systems involve some interaction between nodes (e.g. through participation in the consensus mechanism), but not all DLT systems integrate the kinds of online services that facilitate off-ledger interaction between users that are the defining feature of online platforms. In that sense, equating DLT systems with platforms risks confusing, on the one hand, the technologies and methods that implement the ledger and, on the other hand, the software applications that provide an interface between the ledger and off-ledger activities and other services that support those activities, which raise distinct legal issues. Accordingly, this section of the taxonomy avoids referring to DLT systems as platforms, while acknowledging the prevalence of trade-related DLT-based platforms (i.e. online platforms that use DLT systems to support the delivery of services to users).

## 3. A working definition

11. For the purposes of further legal analysis, a working definition of distributed ledger technology ("DLT") may be formulated in terms of a bundle of technologies and methods[15] that are deployed to implement and maintain a ledger (or database) that is shared, replicated and synchronized on multiple networked computers (or servers).[16] A distributed ledger system ("DLT system") is thus the system (comprised of software and hardware components) that supports the deployment of those technologies and methods. DLT systems differ in their design, governance, purpose and use.

12. At their core, DLT systems represent a new way of recording data. Yet describing DLT systems in such simple terms risks overlooking the potential for DLT systems to support – or indeed transform – trade-related activities. It also risks ignoring the complexity of the technologies involved and the pace at which those

[15] The term "method" is used here in the same sense as it is used, but not defined, in UNCITRAL texts on electronic commerce.

[16] Commentary and legislation often conflate the terms "DLT" and "blockchain" (the original type of DLT system); for consistency, this document uses "DLT system" as an all-encompassing term, while acknowledging that "blockchain" may be a useful shorthand to refer to *any* DLT system.

technologies are developing. Nevertheless, by focusing on data, the trade-related applications of DLT systems may be described as follows:

(a) Data recorded in a distributed ledger may be processed to deliver commercial services. For example, tracking data for goods collected from multiple data providers may be processed as part of a service delivered via a supply chain platform. Supply chain platforms are explored further in the online platforms section of the taxonomy (A/CN.9/1064/Add.3);

(b) Data recorded in a distributed ledger may constitute an identifier for a person, with which the person creates an electronic signature for use in carrying out electronic transactions (e.g. to identify themselves or to sign an electronic record). The use of DLT systems to make use of the UNCITRAL texts dealing with electronic signatures is addressed below (paras. 37–40);

(c) Data recorded in a distributed ledger may constitute a record of a commercial transaction. Some DLT systems employ the term "transaction" in a broader sense to refer to any action that results in a new data entry being submitted to the consensus mechanism,[17] which may not have any connection to a commercial activity, or match the concept of transaction under domestic law;[18]

(d) Data recorded in a distributed ledger may constitute or represent a tradeable "digital asset". For example, data recorded on a distributed ledger might constitute a dematerialized negotiable instrument or represent a unit of cryptocurrency. Digital assets are explored in the digital assets section of the taxonomy (see A/CN.9/1012/Add.3), while the use of DLT systems to make use of the UNCITRAL Model Law on Electronic Transferable Records (MLETR) is addressed below;

(e) Data recorded in a distributed ledger may take the form of computer code which is executed by nodes on the network and which may be programmed to trigger – or be triggered by – an event outside the system (i.e. an "off-ledger" event). An example of such a program is a "smart contract", which is explored in the AI and automation section of the taxonomy (A/CN.9/1012/Add.1).

### 4. Distinguishing the "infrastructure" and "application" layers of DLT systems

13. In effect, DLT systems provide "infrastructure" for trade-related activities, which in turn are enabled by software "applications" that provide an interface between the ledger and off-ledger activities. While the distinction between the infrastructure and application "layers" of DLT systems can be difficult to draw at times, and different layers have been ascribed to DLT systems for different purposes, focusing on the infrastructure of DLT systems and DLT-based applications provides a useful prism through which to identify and analyse the actors involved in the operation of those systems and the legal regimes that are engaged.[19] That distinction is echoed by the observation of the Supreme Court of India in the case of *Internet and Mobile Association of India v. Reserve Bank of India* that there was nothing contradictory between fostering DLT on the one hand and banning certain "by-products" of DLT, namely dealings in cryptocurrencies, on the other hand.[20]

---

[17] For instance, ISO 22739:2020 defines a transaction recorded in a ledger as "the smallest unit of a work process related to interactions with blockchains or distributed ledgers".

[18] For example, laws in almost all states of the United States based on the Uniform Electronic Transactions Act (UETA) define "transaction" to mean "an action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs".

[19] A similar approach is taken by the JIU in its review of blockchain applications: *Blockchain Applications in the United Nations System: Towards a State of Readiness* (JIU/REP/2020/7), box 1.

[20] Supreme Court, *Internet and Mobile Association of India v. Reserve Bank of India*, Writ Petition (Civil) No. 528 of 2018, Judgment, 4 March 2020, [2020] INSC 252, paras. 6.136–6.137. In that case, the court found that the administrative direction banning regulated entities from dealing in cryptocurrencies was unlawful on other grounds.

## C. Actors

14. Depending on the design and purpose of the DLT system, the actors involved in the infrastructure layer may also be involved in the application layer.

### 1. Infrastructure layer

15. The infrastructure layer of DLT systems involves the following actors:

(a) *Developer*: a person or group of persons which designs, develops and maintains the computer code that runs the system;

(b) *Node operator*: a person which operates a node (i.e. a computer that runs the computer code).

16. For some systems, the code that runs the system is not maintained by a single person but rather by an unincorporated and loosely connected community of persons (e.g. open-source community) among whom changes to the code are proposed and reviewed. The outcome of the review determines whether the changes are accepted and later adopted by the node operators.

17. Some DLT systems also involve an *administrator* which controls:

(a) Which persons operate a node, in which case the system is commonly referred to as a "private" system (as opposed to a "public" system); and

(b) Which operations each node performs with respect to the ledger (e.g. reading the ledger, submitting a new data entry to the consensus mechanism, participating in the consensus mechanism), in which case the system is commonly referred to as a "permissioned" system (as opposed to a "permissionless" system).[21]

18. A single person could be the administrator, in which case the DLT system is sometimes referred to as an "enterprise" system. The administrator role could also be performed by a group of persons, in which case the system is sometimes referred to as a "consortium" system (although that term presupposes a certain legal relationship among persons in the group, which is addressed in para. 29 below).[22] As noted above (para. 10), a DLT system could be deployed as an online platform, in which case the administrator might act as the "platform operator". The administrator might also act as the developer for the system and operate or control some or all of the nodes. In effect, the administrator (if any) controls the network that runs the DLT system.

19. Even for systems that do not have an administrator, a person or group of persons may act to advocate the use of a particular DLT system or to promote the development of DLT software.

### 2. Application layer

20. The application layer of DLT systems ushers in a much broader group of actors which participate in the trade-related activities that are supported by the software applications that interact with the ledger. Those actors can be affected by how the system is operated, even if they are not involved in the system's infrastructure. They include persons that transact in the data recorded in the ledger to provide and receive services, as well as persons who transact in digital assets (including cryptocurrency) that are constituted or represented by data recorded in the ledger.

21. Actors involved in the application layer may interact with the ledger by way of an online platform or other online service that is operated by an intermediary, which in turn operates nodes on the network or administers its own network (which may

[21] The terms "permissioned" and "permissionless" are sometimes used to refer to "private" and "public" systems, respectively.

[22] Consortiums may be set up for DLT-related purposes other than the administration and operation of a DLT system, such as advocating DLT use cases or promoting the development of DLT software. Moreover, a consortium may establish a new legal person as a single special purpose vehicle or entity to perform the role of administrator.

itself be hosted on an existing system). For example, persons trading in cryptocurrency may use a third party service or software application (e.g. an exchange or "wallet" service) to submit "transactions" to the ledger, while persons wishing to read or record data in the ledger may use a service delivered via a supply chain platform. Other examples include service providers delivering "blockchain-as-a-Service" (BaaS) solutions, which offer services akin to cloud computing services. Ultimately, how actors interact with the ledger and the roles that they play depend on the design and purpose of the DLT system.

## D. Legal regimes

### 1. Infrastructure layer

#### (a) Contract law

22. A question that commonly arises with respect to the infrastructure layer is how the DLT system is governed. As noted above (para. 3), it is the code that determines what operations each node can perform with respect to the ledger. Nevertheless, the operation of the ledger may be the subject of contractual rights and obligations.

23. Depending on how it is designed, the infrastructure of a DLT system might involve contractual relationships among the node operators and administrators (if any). For example, a contract could exist between the administrator and a node operator, which will establish their legal rights and obligations with respect to the administration of the system, and participation in the network.[23] A contract could exist between a group of persons acting as administrator establishing their legal rights and obligations with respect to the administration of the system.[24] Contractual obligations might address issues such as algorithm testing for the consensus mechanism, node management, and capacity sharing (ensuring that the DLT system performs to a minimum level regardless of the number of participants).

24. A contractual relationship could exist between the administrator and developer establishing their legal rights and obligations with respect to developing and maintaining the code. Even in the absence of an administrator, a limited contractual relationship may exist between the developer and each node operator in the form of a licence (including an open-source licence) establishing the rights and obligations of the node operator with respect to the use of intellectual property in the computer code that runs on the node.

25. It is less likely for a contractual relationship to exist between node operators themselves, particularly if the system lacks the overall control of an administrator (i.e. "public", "permissionless" systems). In the case of *Ruscoe v. Cryptopia Limited (in liquidation)*, the High Court of New Zealand cited with approval the following analysis by the UK Jurisdiction Taskforce (a taskforce of the LawTech Delivery Panel that was established by the Government of the United Kingdom of Great Britain and Northern Ireland, the judiciary of England and Wales, and the Law Society of England and Wales) in its legal statement on digital assets and smart contracts:[25]

> An important feature of some systems is that the rules governing dealings are established by the informal consensus of participants [i.e. nodes], rather than by contract or in some other legally binding way. Consensus rules […] may also determine which version of the distributed ledger is definitive. The rules are

[23] Kelvin Low and Eliza Mik note that node operators in permissionless networks participate "without … agreeing to any system rules or terms of use", while those in permissioned networks are required to "subscribe to system rules" that are synonymous with terms of use of master agreements: "Pause the Blockchain Legal Revolution", *International and Comparative Law Quarterly*, vol. 69, No. 1 (January 2020), pp. 138–140.

[24] In the case of a "consortium" system, the same contract (i.e. the consortium agreement) may address both scenarios.

[25] *Ruscoe v. Cryptopia Limited (in liquidation)*, Case No. CIV-2019-409-000544, Judgment, 8 April 2020, [2020] NZHC 728, para. 21.

self-enforcing in practice, even if not enforceable in law, because only transactions made in compliance with them and duly entered in the ledger will be accepted by participants as valid.[26]

26. However, an administrator of a DLT system may require a particular contractual arrangement to exist as a precondition for participating in the network. Moreover, node operators may contract with one another to trade DLT-based digital assets. So far as the basic operation of a distributed ledger involves the execution of computer code (e.g. a so-called "smart contract") that is programmed to perform part of a contract, additional contract law questions relating to automated contracting arise, which are explored in the AI and automation section (see A/CN.9/1012/Add.1, paras. 23–33, and revisions in A/CN.9/1064/Add.1, paras. 7–18).

### (b) Laws specific to DLT systems

27. Because of the perceived features associated with DLT systems, several jurisdictions have enacted laws that give special legal effect to data that is recorded in a distributed ledger:

(a) In China, the "Rules of Online Litigation issued by the Supreme People's Court" establish a rebuttable presumption in favour of the authenticity of data stored by blockchain technology where that data is adduced as evidence in court proceedings;[27]

(b) In the United States, the "blockchain enabling" law in the state of Vermont makes special provision for the authenticity, admissibility and evidential value of data recorded on a blockchain.[28]

### (c) Other laws

28. It is conceivable that one actor involved in the infrastructure of a DLT system might cause harm to other actors involved in either the infrastructure or application layers of the system. For instance, defective programming by the developer, or defective hardware maintained by a node operator may cause the system to malfunction or otherwise compromise the ledger. In this scenario, tort law may affect the legal rights and obligations among the various actors. The difficulties of establishing liability of developers in tort for damage caused to network participants was highlighted in the case of *Tulip Trading Limited v. Bitcoin Association*.[29] In that case, the High Court of England and Wales found that a claim for breach of tortious and other extracontractual duties by the core developers of several networks running the Bitcoin blockchain, occasioned by a failure to ensure against a loss of control over bitcoin following a hack on the network, did not establish a "serious issue to be tried on the merits".

29. If a group of persons establishes a DLT system as part of a joint venture or in pursuit of a common objective, the law may attach particular legal consequences, including the imposition of extracontractual obligations on each person toward others in the group, beyond the terms of any underlying contract between them (e.g. in the form of a partnership). However, those consequences will likely be more keenly felt in the application layer, when the DLT system is used to support off-ledger activities.

30. Because the basic operation of a distributed ledger involves the recording and transmitting of data, DLT systems potentially engage a range of protective laws with respect to certain types of data or representations of data. Those laws are explored in

[26] UK Jurisdiction Taskforce, "Legal Statement on Cryptoassets and Smart Contracts", November 2019, para. 30. Later on in the legal statement (para. 68), it is observed: "In a fully decentralised system with consensus rules, such as Bitcoin, participants do not undertake any legal obligations to each other".

[27] Interpretation No. 12 of 2021, article 16.

[28] United States, *Vermont Statutes*, title 12, sect. 1913.

[29] High Court of England and Wales, *Tulip Trading Limited v. Bitcoin Association for BSV*, Case No. BL-2021-000313, Judgment, 25 March 2022, [2022] EWHC 667 (Ch).

the data transactions section (see A/CN.9/1012/Add.2 with revisions in A/CN.9/1117). Difficulties may arise in applying those laws on account of obstacles in identifying the operator of a node that processed the data. Moreover, given the geographic distribution of nodes, private international law issues – including questions of applicable law – could arise.

### 2. Application layer

31. The application layer of a DLT system potentially engages a much wider range of legal regimes on account of the variety of trade-related activities that it supports. An activity might be described as "DLT-enabled" or "blockchain-based" even if the preponderant part of the activity takes place off-ledger among persons that are not involved in the operation of the DLT system. Moreover, DLT could be but one of several interoperating technologies and methods that support the activity; indeed, for some activities, a distributed ledger could, at least in principle, be replaced by an alternative method for recording data, such as a centralized database. Against this background, it can be difficult to identify how a particular off-ledger activity interfaces with the ledger itself, and how the DLT system and the data recorded in the ledger is actually used for that activity.

#### (a) Contract law

32. Trade-related activities supported by DLT can involve multiple parties and an assortment of contractual arrangements.[30] The rights and obligations that the various contracts establish will depend on the design of the activity and role that the party plays in that activity, while the types of contractual relationships will depend on the design and purpose of the DLT system.

33. Some contracts will deal specifically with the operation of the underlying DLT system. For instance, a contract could exist between the administrator or node operator (acting as a "node service provider") and an outside application service provider (i.e. a person not participating in the DLT network) which establish rights and obligations with respect to the design and development of a software application to support trade-related activities. If the administrator or node operator itself deploys the application, a contract could exist with a user that establishes rights and obligations with respect to the use of the application that are specifically tailored to the DLT system.

34. Further away from the ledger, if the outside application service provider deploys the software application, the contract that it enters into with the end user of the application could resemble a "traditional" cloud computing contract, specifically those involving the delivery of platform-as-a-service (PaaS) and software-as-a-service (SaaS) solutions. However, even if the contract does not deal with the operation of the underlying DLT system, special provisions might be included in the contract with respect to DLT-specific issues such as (a) limitations on the use and adaptation of open-source software, which could affect the service levels, warranties and indemnities that the application service provider can offer with respect to the software, (b) how data will be fed into and recorded in the ledger, which could have implications for compliance with data privacy, data localization and data security requirements, and (c) limitations on information available regarding the identity and other attributes of other users of the application with whom the user might interact. Moreover, DLT-specific issues may need to be taken into account in applying contract law principles, for instance in the event of a temporary impossibility to perform ("force majeure"), whether that is due to issues with the DLT system itself or "off-ledger" events.

#### (b) Other laws

[30] See, e.g., the description of blockchain applications used by the United Nations system organization in Annex I to the report of the JIU of its review of blockchain applications: footnote 19 above.

35. As noted above (para. 5), laws have been enacted or amended in several jurisdictions to enable or regulate the use of DLT for certain trade-related activities. Those laws primarily concern dealings with digital assets, which are addressed in the digital assets section of the taxonomy (see A/CN.9/1012/Add.3). Laws have also been enacted in some jurisdictions to foster the development of DLT in regulated markets, including through "regulatory sandboxes" that exempt operators from particular laws and regulations.

36. Just as the infrastructure layer of DLT systems engages a range of protective laws with respect to certain types of data or representations of data (see para. 30 above), so too does the application layer, so far as it supports the off-ledger processing of that data. Moreover, so far as data processing takes place via an online platform that interfaces with the ledger (e.g. tracking data processed via a DLT-based supply chain platform), the laws explored in the data transactions section (see A/CN.9/1012/Add.2 with revisions in A/CN.9/1117) will also be engaged.

## E. Relevant UNCITRAL texts

### 1. Electronic commerce texts

37. A distributed ledger implemented by a DLT system might record data that forms part of an electronic transaction or an electronic communication. To that end, UNCITRAL electronic commerce texts apply to give legal recognition to the use of that data.

38. Owing to the technology neutral approach taken to their drafting, UNCITRAL electronic commerce texts can give legal effect to the methods used by DLT systems to provide assurances as to the qualities of the data recorded in the distributed ledger, including through the provision of trust services. As noted above, 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 with notions of "integrity" under UNCITRAL electronic commerce texts:

(a) Article 8 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. Accordingly, a DLT system can be used to meet requirements regarding the presentation and retention of originals applying the functional equivalence rule in article 8;

(b) While integrity of data to which an electronic signature is applied is not a function of electronic signatures under UNCITRAL electronic commerce texts, article 6(3)(d) MLES acknowledges that national laws may require paper-based signatures and seals to assure the integrity of the information to which they relate, and provides that an electronic signature may fulfil that function by detecting any alteration to that information after the time of signing;

(c) Under article 10 MLETR, integrity is one of the functions that a data message in the form of an electronic record must fulfil in order to be an electronic transferable record that is legally equivalent to a paper-based transferable document or instrument. Like the MLEC, the MLETR provides that the function is fulfilled if the information contained in the electronic record, has remained "complete and unaltered" apart from any change which arises in the normal course of communication, storage and display.

[*Section to be updated subject to consideration by the Commission of the draft Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services (see A/CN.9/1112).*]

39. Moreover, UNCITRAL electronic commerce texts subject the methods, which are used to satisfy functional equivalence rules, to a requirement of reliability. While reliability depends on the circumstances in which the underlying data is being used, other perceived features of the DLT system, notably the auditability and security of the data recorded in the ledger, will likely be relevant factors in assessing the reliability of the methods supported by the DLT system to assure the qualities of data recorded in the ledger.

40. It follows that UNCITRAL electronic commerce texts are not only compatible with the use of DLT systems in trade, but also enable the provision of DLT-enabled trade-related services. This is demonstrated by the fact that a significant number of pilot projects being designed and deployed to support the issuance and use of electronic transferable records under the MLETR rely on DLT-enabled services provided via online platforms.

### 2. Secured transactions texts

41. DLT systems can be used to support dealings in digital assets that purport to represent security interests in off-ledger assets. Separately, a person might wish to create security interests in a digital asset. An appraisal of the application of the UNCITRAL Model Law on Secured Transactions (MLST) in those scenarios is contained in the digital assets section of the taxonomy (see A/CN.9/1012/Add.3, paras. 37–38). Moreover, a DLT system could be deployed to support the operation of the registry under the MLST (e.g. the distributed ledger could constitute the registry record).[31]

### 3. Dispute resolution texts

42. As noted above (para. 10), DLT systems are used to support the delivery of services constituting an online platform, which could comprise dispute resolution services. An appraisal of the application of UNCITRAL dispute resolution texts to online dispute resolution platforms is contained in the online platforms section of the taxonomy (see A/CN.9/1064/Add.3, paras. 41–49).

### 4. Insolvency texts

43. An appraisal of the application of UNCITRAL model laws on insolvency to DLT-based digital assets is contained in the digital assets section (see A/CN.9/1012/Add.3, paras. 39–42).

[31] See, e.g., World Bank, *Distributed Ledger Technology & Secured Transactions: Legal, Regulatory and Technological Perspectives – Guidance Notes Services* (Washington, 2020).