UNCITRAL | UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAW

Taxonomy of legal issues related to the digital economy

Prepared by the secretariat of the United Nations Commission on International Trade Law

UNITED NATIONS

Further information may be obtained from:

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

Telephone: (+43-1) 26060-4060
Telefax: (+43-1) 26060-7-4060
Internet: uncitral.un.org
Email: uncitral@un.org

UNITED NATIONS COMMISSION ON INTERNATIONAL TRADE LAW

Taxonomy of legal issues related to the digital economy

Prepared by the secretariat of the United Nations Commission on International Trade Law

UNITED NATIONS
Vienna, 2023

Note

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

UNITED NATIONS PUBLICATION
Sales No.: E.12.V.11
ISBN 978-92-1-002939-1
e-ISBN 978-92-1-358505-4

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

This publication has not been formally edited.

Publishing production: English, Publishing and Library Section, United Nations Office at Vienna.

Contents

Abbreviations and acronyms

AI	Artificial intelligence
CISG	United Nations Convention on Contracts for the International Sale of Goods
DLT	Distributed ledger technology
ECC	United Nations Convention on the Use of Electronic Communications in International Contracts
EU	European Union
HCCH	Hague Conference on Private International Law
ISO	International Organization for Standardization
ITU	International Telecommunication Union
MAL	UNCITRAL Model Law on International Commercial Arbitration
MLEC	UNCITRAL Model Law on Electronic Commerce
MLES	UNCITRAL Model Law on Electronic Signatures
MLETR	UNCITRAL Model Law on Electronic Transferable Records
MLIT	UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services
MLST	UNCITRAL Model Law on Secured Transactions
MSME	Micro, small and medium enterprise
New York Convention	Convention on the Recognition and Enforcement of Foreign Arbitral Awards
OECD	Organisation for Economic Co-operation and Development
Singapore Mediation Convention	United Nations Convention on International Settlement Agreements Resulting from Mediation
UNCITRAL	United Nations Commission on International Trade Law
UNCTAD	United Nations Conference on Trade and Development
UNIDROIT	International Institute for the Unification of Private Law
WTO	World Trade Organization

UNCITRAL texts are available at uncitral.un.org

Introduction

A. About this taxonomy

1. The idea of creating a taxonomy of legal issues related to the digital economy developed out of exploratory work carried out by the United Nations Commission on International Trade Law (UNCITRAL) secretariat to identify topics for possible future work by UNCITRAL to address the applications of emerging digital technologies in trade.[1] This taxonomy serves both as a record of that exploratory work and as a map to guide the development of proposals for legislative work to fill gaps in existing law.

2. The taxonomy addresses the following topics: (i) artificial intelligence; (ii) data; (iii) digital assets; (iv) online platforms; and (v) distributed ledger systems. For each topic, the taxonomy:

- Defines *key concepts* in legal terms
- Explores the *actors, legal relationships* and *legal issues* involved in the deployment and use of associated technologies and applications
- Appraises the application of existing *UNCITRAL texts*.

3. Consistent with UNCITRAL practice, the taxonomy covers commercial relations in general. It therefore does not focus on regulation of specific relationships (e.g., trade with weaker parties, such as "consumers" or MSMEs) or types of transactions (e.g., trade in particular markets or in particular items of trade). Nor does it focus on legal issues related to privacy and data protection or to intellectual property, for which the implications of digital trade are being addressed in other international forums, including the Council of Europe and World Intellectual Property Organization.

4. The taxonomy has been prepared in view of the central and coordinating role of UNCITRAL within the United Nations system in addressing legal issues related to the digital economy and digital trade. It draws on the work of other organizations within the United Nations systems, particularly the United Nations Conference on Trade and Development (UNCTAD) and the International Telecommunication Union

[1] The exploratory work itself stems from a decision by UNCITRAL in 2018 requesting the secretariat to "compile information on legal issues related to the digital economy": *Official Records of the General Assembly, Seventy-third Session, Supplement No. 17* (A/73/17), para. 253(b). A progress report prepared by the UNCITRAL secretariat in 2020 provides additional background to the development of the taxonomy: see A/CN.9/1012, paras. 10-12.

(ITU).[2] It has also been finalized in consultation with the Hague Conference on Private International Law (HCCH) and the International Institute for the Unification of Private Law (UNIDROIT), which have been exploring legal aspects of the digital economy within the scope of their respective mandates, notably with respect to digital assets and financial products.

5. Preliminary drafts of the various parts of the taxonomy were developed incrementally and submitted to UNCITRAL for consideration. In 2022, UNCITRAL authorized the publication of those parts of the taxonomy. At the same time, it was noted that, by its nature, the taxonomy is a "living document" and that further revisions could be anticipated (A/77/17, para. 165).

B. About UNCITRAL and its work on digital trade

6. UNCITRAL – the United Nations Commission on International Trade Law – is the core legal body of the United Nations system in the field of international commercial law. Established by the General Assembly, the mandate of UNCITRAL is to further the progressive harmonization and modernization of the law of international trade, which it pursues by preparing and promoting the use and adoption of legislative and non-legislative instruments in various areas of commercial law. One of these areas is electronic commerce – or "digital trade" – in which UNCITRAL has prepared a suite of model laws and a treaty. These texts, which have been developed by UNCITRAL Working Group IV on electronic commerce to enable and facilitate the use of electronic means to engage in commercial activities, have been adopted in over 100 States worldwide.

7. UNCITRAL electronic commerce texts are predominantly concerned with communications between commercial parties by means of "data messages" (i.e. by electronic, magnetic, optical or similar means). Earlier texts, such as the 1996 UNCITRAL Model Law on Electronic Commerce (MLEC), were prepared with particular reference to electronic communications by means of use of electronic data interchange (EDI), while later texts, such as the 2005 United Nations Convention on the Use of Electronic Communications in International Contracts (ECC), were prepared with a view to electronic communications taking place using Internet technologies.

8. Since then, technological developments have dramatically transformed international trade, creating new ways of trading and new items of trade. While more recent UNCITRAL electronic commerce texts, notably the 2017 Model Law on Electronic Transferable Records (MLETR) and 2022 Model Law on the Use and Cross-border

[2] UNCITRAL Working Group IV on electronic commerce has recognized the utility of maintaining consistency with ITU terminology in legislative work on digital trade: see, e.g., A/CN.9/1005, para. 86.

Recognition of Identity Management and Trust Services (MLIT), have moved to recognize digital items of trade and to facilitate the use of distributed systems, other topics for future harmonization efforts were presented at a congress organized in 2017 to mark the fiftieth anniversary of UNCITRAL and to explore new directions in cross-border commerce. Thus, when UNCITRAL was ultimately presented with a proposal to closely monitor developments relating to the legal aspects of smart contracts and artificial intelligence (A/CN.9/960), it was decided that the exploratory work to be carried out by the secretariat should proceed on a "broader understanding of the legal issues related to the digital economy", encompassing other topics such as the use of distributed ledger technology, supply chain management and cross-border data flows. These perspectives have framed not only the development of this taxonomy, but also proposals for preparatory work by UNCITRAL on new legislative and non-legislative texts on digital trade.

Part one.

Artificial intelligence

A. Relevance to international trade

9. The increased and expanding use of artificial intelligence (AI) is transforming the global economy. By one forecast, cited in the 2019 *Digital Economy Report* published by UNCTAD, AI could generate additional global economic output of around $13 trillion by 2030, contributing an additional 1.2 per cent to annual global growth in gross domestic product.[3] Thanks to the availability of large quantities of data, improvements in processing power and advanced algorithms, AI is being used by traders to develop and deploy software and hardware systems that represent the next generation of automation (sometimes referred to "intelligent automation"). AI is transforming trade not just in terms of new products and services being traded, but also in terms of increased efficiencies in trade-related activities such as supply chain management, the marketing of goods and services (including via online platforms), and the formation and performance of contracts.

B. What is artificial intelligence?

10. The term "artificial intelligence" refers both to (i) the capability of a machine to exhibit or simulate intelligent human behaviour, and (ii) a branch of computer science concerned with this capability.[4] Only the first meaning is relevant in the trade context, where the term AI "system" is often used (comprised of software and hardware components delivering that capability). In this regard, it is important to acknowledge that the technology driving the capability of AI systems is still in its infancy and

[3] UNCTAD, *Digital Economy Report 2019: Value Creation and Capture – Implications for Developing Countries* (Geneva, 2019), p. 8, referring to ITU, "Assessing the Economic Impact of Artificial Intelligence", Issue Paper, No.1 (Geneva, September 2018).

[4] See John McCarthy, *What is Artificial Intelligence?*, revised, 12 November 2007, available at www-formal.stanford.edu/jmc/whatisai.pdf. This dual meaning is recognized by ISO, which defines the term "artificial intelligence" to mean: (i) "an interdisciplinary field, usually regarded as a branch of computer science, dealing with models and systems for the performance of functions generally associated with human intelligence, such as reasoning and learning"; and (ii) the "capability of a functional unit to perform functions that are generally associated with human intelligence such as reasoning and learning": ISO, *Information Technology – Vocabulary*, ISO/IEC Standard No. 2382, 2015.

disagreement exists among computer scientists as to what constitutes the "intelligent" behaviour to be exhibited or simulated by these systems.

11. Nevertheless, several international and regional initiatives have sought to define the general contours of AI systems.

- The Council of the OECD adopted a recommendation on AI in 2019 ("OECD AI Recommendation")[5] which defines "AI system" as "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments". The definition adds that AI systems are "designed to operate with varying levels of autonomy".
- The General Conference of UNESCO adopted a recommendation on the ethics of AI in 2021 ("UNESCO Recommendation")[6] with a view to "strengthen[ing] the elaboration and implementation of national and international legislation, policies, and strategies in the field of AI". The recommendation describes AI systems as "information-processing technologies that integrate models and algorithms that produce a capacity to learn and perform cognitive tasks leading to outcomes such as prediction and decision-making in material and virtual environments". Like the OECD AI Recommendation, it acknowledges that "AI systems are designed to operate with varying degrees of autonomy by means of knowledge modelling and representation and by exploiting data and calculating correlations". Moreover, the recommendation expressly eschews the ambition to provide a single definition of AI by reference to the technologies or techniques used, noting that "such a definition would need to change over time", although it does single out "machine learning" and "machine reasoning".
- In the European Union, the European Parliament adopted two resolutions in 2020 requesting the European Commission to propose regulations on (i) the ethical use and governance of AI and (ii) a civil liability regime for AI.[7] To that end, the resolutions define an "AI system" as a software-based system, or a system embedded in hardware devices, that "displays behaviour simulating intelligence" by "collecting and processing data, analysing and interpreting its environment, and by taking action, with some degree of autonomy, to achieve specific goals". The European Commission subsequently issued a proposed regulation addressing the ethical use

[5] OECD, Recommendation of the Council on Artificial Intelligence (2019), document C/MIN(2019)3/FINAL.

[6] UNESCO, *Records of the General Conference, Forty-first Session, Resolutions* (Paris, 2022), resolution 34 and annex VII.

[7] European Parliament, Resolution of 20 October 2020 with Recommendations to the Commission on a Framework of Ethical Aspects of Artificial Intelligence, Robotics and Related Technologies (2020/2012(INL)); European Parliament, Resolution of 20 October 2020 with Recommendations to the Commission on a Civil Liability Regime for Artificial Intelligence (2020/2014(INL)).

> and governance of AI, which defines an "AI system" in similar terms to the OECD AI Recommendation – "software [that] can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing real or virtual environments". Unlike the OECD AI Recommendation and the resolutions of the European Parliament, the definition in the proposed regulation is limited to AI systems that are developed using specific technologies and techniques, notably "machine learning approaches", "logic- and knowledge-based approaches", and "statistical approaches".[8]

12. Based on the instruments outlined above, an AI system is essentially a type of automated system (also known as an "electronic agent") that is already addressed in legislative texts prepared by UNCITRAL and in legislation enacted in many jurisdictions governing the use of automation in commercial and administrative activities. In that context, automated systems are generally understood to mean software systems that are programmed to perform pre-defined tasks without human involvement. Like automated systems, AI systems essentially involve the output of data messages (capable of being reproduced in the form of sound, images or text) which are generated by processing data collected from a variety of inputs (i.e. data sources).

13. However, the tasks referred to in these instruments (e.g., making "predictions", "recommendations" and "decisions") suggest that AI systems are more complex and capable than the automated systems contemplated in existing law. Two features are commonly put forward to distinguish AI systems from other automated systems. The first feature is that, rather than simply performing predefined tasks, AI systems use methods or techniques that improve the performance of these task, and allow for the performance of new tasks according to pre-defined objectives in a "non-deterministic" or stochastic manner. The second feature is that AI systems have the capacity to process large quantities of data from multiple sources (sometimes referred to as "big data"). These two features have in turn led to AI systems being described as "autonomous", "unpredictable" and "opaque".

14. The "unpredictability" and "opaqueness" of AI systems can be relevant in applying existing legal regimes to the operation of AI systems, as discussed below. However, it is questionable whether such qualitative and subjective features should serve as a basis for a working definition of "AI" for the purposes of further legal analysis. It is also questionable whether a working definition should import loaded human analogies such as "autonomy" which, as with the concept of "intelligence" itself is difficult to define in a machine context. Moreover, in keeping with the principle of technology neutrality, such a working definition should avoid reference to the specific types of

[8] See European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts, document COM(2021) 206 final (21 April 2021).

methods or techniques that are used. It follows that conceptualizing an "AI system" as a type of automated system – i.e. a software system programmed to perform without human intervention – still serves as a basis for formulating a working definition for the purposes of further legal analysis.

C. Actors

15. The OECD AI Recommendation defines AI actors as those who play an active role in the "AI system lifecycle". This is defined to consist of four phases: (i) design, data and models; (ii) verification and validation; (iii) deployment; and (iv) operation and monitoring. The OECD AI Recommendation also refers to "stakeholders", which comprise those AI actors as well as other persons involved in or affected by an AI system. For its part, the UNESCO Recommendation defines AI actors as any actor involved in at least one stage of the AI system life cycle, which ranges from research, design and development to deployment and use.[9]

16. Based on these instruments, the use of an AI system (as with the use of other automated systems) involves the following actors:

- *Developer* – the person who designs, programs and verifies the software, and integrates it with external hardware, applications and data sources before deployment.
- *Data provider* – the person who provides data to the system (e.g., data needed to support the development or operation of the system).
- *Deployer* – the person who integrates the system into existing business operations (e.g., the supply of goods and services), including by setting up, managing, maintaining and supporting the supply of data and infrastructure necessary for the operation and monitoring of the system and its interaction with the supplied data once deployed.
- *Operator* – the person who operates the system. In many cases, the operator will be the person who deploys the system. In the case of AI-enabled goods or services, the operator of the system will not generally be the end user of the goods or service, even if the end user exercises control over how and when the system performs (e.g., through data inputs).
- *Affected person* – any other person affected by the operation of the system, including the end user of AI-enabled goods or services or person interacting with the system through the use of another machine.

[9] UNESCO Recommendation, para. 2(b).

D. Legal regimes

1. Introduction

17. Owing to its widespread use in many sectors of society, AI engages a wide range of laws, including laws dealing with privacy and data protection, human rights (including anti-discrimination), employment and competition. In the areas of private law that are more closely connected to trade, the disruptive effects of AI are felt more keenly in the operation phase of the AI lifecycle. This is not to say that particular legal issues are not engaged in earlier phases, such as in the development of AI systems.

- For instance, in 2018, the Ministry of Economy, Trade and Industry of Japan published contract guidelines on the utilization of AI (hereafter the "METI AI Guidelines") in response to the "many legal issues regarding the development and utilization of AI-based software" as between developers (referred to as "vendors" of AI software) and deployers (referred to as "users" who apply the software to their business).[10]

18. In the trade context, a rough distinction may be drawn between the use of AI **in trade** – for example, through the supply of AI-enabled goods and services – and the use of AI **to trade** – for example, through the use of AI systems to manage supply chains (including inventory forecasting), to market goods and services (including via online platforms), and to enter into and perform contracts. While this distinction is not always clear-cut, it nevertheless serves as a useful tool for analysing the legal issues related to the use of AI.

2. AI in trade

Contract law

19. Where AI is used in trade, a contractual relationship may exist between the person developing the AI system and the person deploying or operating the system (e.g., a contract for the development of an AI system) or between the person operating the AI system and an affected person (e.g., an end-user agreement for the supply of AI-enabled services). In both of these cases, the distinguishing features of AI (as identified in section B above) can present difficulties in applying existing contract law rules, particularly with regard to establishing the existence of breach of contract and establishing causation of harm arising from the use of the AI system.

[10] Japan, Ministry of Economy, Trade and Industry, *Contract Guidelines on Utilization of AI and Data: AI Section* (June 2018).

- Lack of information about the algorithm running an AI system and the data processed may make it difficult for a party claiming breach to establish a correlation between the inputs and outputs of the system (sometimes referred to as the "black box" problem). For instance, the difficulty may be in establishing whether the party providing the AI-enabled service has performed what it undertook to perform according to the terms of the contract. The issue is compounded by contracts framing performance parameters (as that term is used in the Notes on the Main Issues of Cloud Computing Contracting[11]) in broad terms.
- Lack of information may also make it difficult for the party to establish that the breach was the cause of harm for the purposes of establishing contractual liability. For instance, the difficulty may be in establishing whether damage or injury suffered was caused by the operation of the AI system itself, as opposed to the quality of the data processed by the AI system that is provided by a third party (or indeed by the party claiming breach).

20. These difficulties have the potential to shift the balance between contracting parties in the traditional sale context by putting the seller/supplier in a stronger position vis-à-vis the purchaser. Proposals have been put forward for rebalancing through education of the parties (e.g., the development of model contract provisions and good practice guides). In addition, proposals for legislative intervention to impose additional obligations on the operator of the AI system to comply with an emerging body of standards on the ethical use of AI may also have a rebalancing effect, even if those proposals and standards are not specifically addressed to the trade context.[12]

Tort law

21. Similar evidentiary difficulties regarding causation of harm arising from the use of an AI system may arise in the context of existing tort law, particularly where the allegedly tortious conduct is constituted by a person operating the AI system. For instance, it may be difficult to establish that the output of the AI system was caused by a failing in how the system was programmed, rather than an erroneous input from an external data source or third-party interference with the system. These difficulties may be magnified by the multiplicity of actors involved in the development and operation of AI systems. A 2019 report by an expert group set up by the European Commission to assist in developing guiding principles for the possible adaptation of laws within the European Union (the "EU Expert Group on Liability and New Technologies") restates these difficulties in the following terms:

[11] See https://uncitral.un.org/cloud.

[12] A snapshot of international initiatives is provided in the Secretary General's *Road Map for Digital Cooperation*, A/74/821, paras. 53-57.

> Hard as it is to prove that some hardware defect was the reason someone was injured, for example, it becomes very difficult to establish that the cause of harm was some flawed algorithm. [...] It is even harder if the algorithm suspected of causing harm has been developed or modified by some AI system fuelled by machine learning and deep learning techniques, on the basis of multiple external data collected since the start of its operation.[13]

It has been suggested that, while these difficulties may not be insurmountable, they may add to the cost and time of dispute resolution.[14]

22. Additional difficulties may arise where the allegedly tortious conduct is constituted by the output of the AI system itself.[15] For instance, the output of an AI system may constitute a false, misleading or defamatory statement, a breach of copyright or the disclosure of confidential information, in which case questions arise as to the person to whom the output of the AI system can be attributed (see further discussion on the issue of attribution under the heading "contract formation" below). If liability depends on the state of mind of the tortfeasor (i.e. fault-based liability), additional questions arise as to when and how that state of mind is to be assessed (e.g., what the person "knew", "believed" or "intended" in connection with the output of the system). Questions may also arise regarding the standard of conduct against which the tortfeasor is to be assessed for the purpose of applying tort law principles (e.g., the standard of reasonableness).[16] In that regard, the emerging body of standards on the ethical use of AI may be relevant.[17]

23. Difficulties in applying existing tort law rules have the potential to disadvantage affected persons, who may suffer harm as a result of the operation of AI systems. In response, various proposals have been put forward to establish new liability regimes to better balance the interests of the actors involved in the use of AI systems. One proposal is to subject the operation of AI systems to strict liability rules, similar to those which apply to defects under product liability regimes. Several reasons have been put forward for this approach: (i) it encourages actors engaged in dangerous activities to take necessary safeguards and to carry out those activities with utmost care; (ii) it places the costs of such activities on those who benefit the most from them; and (iii) it protects those actors who are potentially affected by such activities

[13] *Liability for Artificial Intelligence and other Emerging Digital Technologies*, 2019. Similar difficulties were identified by the SecretaryGeneral's High-level Panel on Digital Cooperation: *The Age of Digital Interdependence*, June 2019, p. 25.

[14] Lord Sales, *Algorithms, Artificial Intelligence and the Law*, Sir Henry Brooke Lecture delivered at the Freshfields Bruckhaus Deringer, London, 12 November 2019, pp. 12–13.

[15] Compare this to attribution of "loss", as discussed by the EU Expert Group on Liability and New Technologies, which is a matter of causation: *Liability for Artificial Intelligence and other Emerging Digital Technologies*, 2019.

[16] As the EU Expert Group on Liability and New Technologies noted, "[e]merging digital technologies make it difficult to apply fault-based liability rules, due to the lack of well-established models of proper functioning of these technologies and the possibility of their developing as a result of learning without direct human control": *Liability for Artificial Intelligence and other Emerging Digital Technologies*, 2019, p. 23.

[17] See footnote 12 above.

and compensates them adequately – in particular, it avoids the need for an affected person to seek compensation from multiple parties in proportion to their contribution to the harm.

24. Another proposal is to introduce a no-fault compensation scheme for accidents involving AI systems, backed by mandatory insurance and a fall-back public fund.[18] While it is conceivable for such a scheme to be implemented for some AI systems such as AI-enabled goods distributed locally, additional challenges may be presented in relation to other AI systems, particularly AI-enabled services delivered online to global users.

25. Yet another proposal is to adapt the law and principles of agency to the relationship between the AI system and its operator. However, it has been noted that differences in the law of agency between different jurisdictions may make it difficult to find harmonized solutions, particularly in the absence of agreed standards of conduct.[19] Likening an AI system to an "agent" conjures up calls, so far not taken up, to confer separate legal personality on AI systems. Indeed, the various proposals outlined so far assume that AI systems remain mere "tools" that have no independent will or legal personality.

26. Short of introducing new liability regimes, other proposals have been put forward to supplement existing tort law rules, including by shifting the burden of proof in establishing tort claims, subjecting AI systems to an independent *ex ante* review,[20] evaluating the need to prevent contractual limitation of liability,[21] or imposing new obligations of disclosure on the person deploying or operating an AI system.[22] Some of these proposals draw on the emerging body of standards on the ethical use of AI. For instance, the UNESCO Recommendation acknowledges that the principle of transparency (as to the operation of AI systems) is "necessary for relevant national and international liability regimes to work effectively".[23]

27. The various proposals outlined above raise the question as to whether all AI systems should be treated equally, or whether new liability regimes should apply only

[18] See, e.g., European Parliament, Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)).

[19] See EU Expert Group on Liability and New Technologies, *Liability for Artificial Intelligence and other Emerging Digital Technologies*, 2019, p. 25.

[20] The Secretary-General's High-level Panel on Digital Cooperation recommended that "[a]udits and certification schemes should monitor compliance of [AI] systems with engineering and ethical standards": *The Age of Digital Interdependence*, June 2019, recommendation 3C.

[21] European Parliament, Resolution of 20 October 2020 with Recommendations to the Commission on a Civil Liability Regime for Artificial Intelligence (2020/2014(INL)).

[22] See, e.g., key findings 22, 24, 26 and 27 of the European Union Expert Group on Liability and New Technologies: *Liability for Artificial Intelligence and other Emerging Digital Technologies*, 2019, pp. 7–8.

[23] UNESCO Recommendation, para. 34.

to some types of AI systems. A further question arises as to how to differentiate AI systems in a manner that promotes legal certainty and predictability.

- The EU Expert Group on Liability and New Technologies found that a strict liability regime may be appropriate for AI systems that cause "significant harm", where the significance of the harm is determined by reference to the potential frequency and severity of harm.
- In its 2020 resolution for a civil liability regime for AI, the European Parliament similarly called for a strict liability regime to be established for "high risk" AI systems, which it defines as "a significant potential [...] to cause harm or damage to one or more persons in a manner that is random and goes beyond what can reasonably be expected".

Product liability law

28. Many legal systems have special regimes for product liability. A question arises as to how the use of AI systems in trade engages liability under these regimes. Product liability laws may be restricted to goods and exclude services. Accordingly, while these regimes may apply to AI-enabled goods, they may not apply to AI-enabled services. Moreover, product liability laws may only cover certain types of harm (e.g., personal injury and property damage) and only certain types of products (e.g., products for personal, family or household use). As such, these laws may be of limited applicability in the trade context.

29. Another issue is that product liability regimes assume that the product does not change over time. Most product liability regimes provide for an exception to liability in circumstances where the product was developed in accordance with the knowledge and technology at the time of production. Also, product liability laws usually exclude liability if the defect did not exist when the product was put into circulation. This may pose challenges in establishing liability for AI systems, particularly those that run on machine learning.

3. AI to trade

30. The use of AI to trade primarily raises issues of contract law. In particular, novel issues may be engaged by the use of AI systems in the formation and performance of contracts. Given its reliance on data, the use of AI systems also raises legal issues related to data processing, which are addressed in part two of this taxonomy. Other legal regimes may be engaged by the use of AI systems to perform contracts, particularly where those contracts create or assign property rights, including security rights.

Dealing with "smart contracts"

31. Some of the contract law issues associated with the use of AI – and automation more broadly – have been viewed through the prism of "smart contracts".

32. When originally coined, the term "smart contract" was conceived of as "a computerized transactions protocol that executes the terms of a contract".[24] More recently, the term has become closely associated with DLT systems, where "smart contracts" are used to automate transactions on a distributed ledger without any necessary connection between the transaction and the formation or performance of a contract. For instance, the ITU recommendation on the requirements for DLT systems defines "smart contract" to mean a "program written on the distributed ledger system that encodes the rules for specific types of distributed ledger system transactions in a way that can be validated, and triggered by specific conditions",[25] while ISO defines it as a "computer program stored in a DLT system wherein the outcome of any execution of the program is recorded on the distributed ledger".[26] Conversely, legal doctrine, as well as legislation in some jurisdictions, employ the term – or the variant "smart legal contract" – to refer specifically to a computer program that embodies or performs a contract. Legal doctrine also makes the point that the term "smart contract" is a misnomer in that it refers to programs that are neither "contracts" nor "smart" (in the sense of exhibiting "intelligent" behaviour within the meaning of AI).

33. At the very most, a "smart contract" is a program used to perform a contract in an automated manner. At the very least, it is a program used to perform a task in an automated manner without any connection to a contract. To avoid confusion, and in keeping with the principle of technology neutrality, this taxonomy does not use the term "smart contract", and instead refers to the use of automated systems – however deployed – in the formation and performance of contracts.

Contract formation

34. Contracts are formed by expressions of will (e.g., offer and acceptance) that evidence an agreement between persons. AI systems may operate to generate or process data messages which purport to constitute an offer or an acceptance. Automated systems are widely used to transact, whether with human involvement (e.g., a natural person interacting with an automated system via a website or e-commerce platform) or without. Examples of automated contracting include (i) supply contracts formed

[24] Nick Szabo, "Smart Contracts", 1994, available at www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.

[25] ITU, *Requirements for Distributed Ledger Systems*, Recommendation ITU-T F.751.0, 13 August 2020, para. 3.2.16.

[26] ISO, *Blockchain and Distributed Ledger Technologies — Overview of and Interactions between Smart Contracts in Blockchain and Distributed Ledger Technology Systems*, ISO/TR 23455:2019.

by electronic communications sent between computers using electronic data interchange, (ii) sales contracts formed by a natural person placing an order through a website (interacting with the automated system operating "behind" the website), (iii) contracts formed by "smart" devices placing orders via connected online platforms, and (iv) contracts formed by Internet bots interacting with websites (e.g. "screenscraping bots" and "shopping bots").

35. The use of *automated* systems generally to form a contract raises several issues, including (i) the legal validity of the contract, (ii) identifying the parties to the contract, (iii) determining the intention of the parties to be bound (and other matters relating to state of mind) and (iv) identifying the terms of the contract.

- In many jurisdictions, the law recognizes that a contract may be formed by the exchange of data messages (i.e. electronic contracts). Some also expressly recognize that a contract may be formed by the interaction of automated systems (or "electronic agents") without human involvement. For instance, courts have upheld contracts formed via a website or other software system operated by a party without any human intervention of that party. Courts have also upheld contracts involving the interaction of two machines (e.g., an Internet bot deployed by one party interacting with the website operated by another party, or a contract formed by two computer programs deployed on an online trading platform).
- Recalling the assumption that AI systems are mere "tools" with no independent will or legal personality of their own, applicable law will determine the person to whom the output is to be attributed, and thus the identity of the party to the contract formed by that output.
- For instance, in a 2022 judgment concerning the "inventor" of an invention generated by the output of an AI system for the purposes of patent law, the Federal Court of Australia highlighted that the attribution was a "question of law", and observed that matters relevant to determining the person to whom the invention is to be attributed might include ownership of copyright in the computer code, ownership of the computer running the code, and responsibility for the operation and maintenance of the system.[27]
- Applicable law will also determine whether the output of an automated system can be characterized as an expression of will, particularly if the party to whom that output is attributed is unaware of the circumstances of the conclusion of the contract, or that a contract has even been concluded. If the contract is formed via an online platform, the terms of use for the platform may be relevant so far as they evidence the prior consent of the party as to how

[27] *Commissioner of Patents v. Thaler*, File No. VID 496 of 2021, Judgment, 13 April 2022, [2022] FCAFC 62.

the platform may be used to form contracts. The use of automated systems to form contracts may engage other contract law rules (e.g., the law of mistake) which require a determination of a party's state of mind (e.g., what a party "knows", "believes" or "intends" in connection with the output of the system). These rules may require state of mind to be determined subjectively (i.e. what the person actually knows, believes or intends) or objectively (i.e. what the person ostensibly knows, believes or intends, based on the circumstances).

- The *Quoine* case in Singapore provides an example of how the law of mistake can be applied to a contract formed by the interaction of computer programs without human intervention or knowledge of the parties that the contract had been concluded.[28]

- A question may arise as to the validity and interpretation of a contract that is memorialized in computer code. As code is a form of data message, the validity of contracts memorialized in code may already be covered by laws that recognize electronic contracts. A question may also arise as to whether the contract is sufficiently certain and complete to be valid or enforceable, particularly if it depends on "dynamic information" based on an external data source that may change periodically or continuously, such as a market price.

36. It has been suggested that addressing these issues may be more challenging in the context of *AI* systems.

- Writing extrajudicially, one judge of the Supreme Court of the United Kingdom has queried the ability of English contract law to deal with these issues in cases involving AI systems using machine learning techniques that "autonomously generate transactions":

  If there is to be a contract drafted or adapted by machines, there will have to be significant development to our law of contract which will require careful and imaginative consideration. […] Questions about the intention to enter into legal relations, to whom that intention is to be attributed and how the terms of a computer-generated contract are to be recorded to achieve legal validity and interpreted will require innovative thinking.[29]

- In the *Quoine* case, the Court of Appeal of Singapore stressed on several occasions that the automated system was programmed to operate in a "deterministic" manner. While the court did not indicate whether its legal analysis of contract law – specifically, the law of mistake – would have differed if the system had not been programmed to operate in a "deterministic" manner but rather "to develop its own responses to varying

[28] Singapore, *Quoine Pte. Ltd. v. B2B2 Ltd.*, Civil Appeal No. 81 of 2019, Judgment, 24 February 2020, *Singapore Law Reports*, vol. 2020, No. 2, p. 20, [2020] SGCA(I) 02.

[29] Lord Hodge, *The Potential and Perils of Financial Technology: Can the Law Adapt to Cope?*, Edinburgh FinTech Law Lecture delivered at the University of Edinburgh, 14 March 2019.

conditions", it has been suggested in legal doctrine that, based on the judgment in that case, such systems may require a different approach.

Contract performance

37. To the extent that an automated system is used to perform a contract (e.g., the original use case for "smart contracts"), one issue is how the terms of the contract can be translated into the code of the computer program that runs the system. Particular attention has been drawn in legal doctrine to "soft" concepts such as "reasonableness" and "good faith", which generally depend on the circumstances at the time of performance, and which may be beyond what was contemplated at the time that the code was written. The issue is primarily a matter of coding that raises the question as to whether the operation of the program as coded satisfies the terms of the contract (or regulatory requirements). Rather than raising novel questions of contract law, the issue raises questions regarding the liability of the developer for failing to correctly translate the terms of a contract into code, whether in tort or in contract (e.g., for breach of its contract with the operator).

- In the Russian Federation, amendments to the Civil Code in 2019 introduced a provision that expressly recognizes the use of automation to perform contracts.[30]

38. Another issue that has been raised is remedies. The case commonly cited is that of a "smart contract" deployed in a DLT system whose performance cannot be altered or stopped once deployed. It is conceivable that a court seized of a dispute in that case would have a range of remedies at its disposal from which to choose to best resolve the dispute and to provide adequate relief for the injured party. Nevertheless, questions have been raised in legal doctrine as to whether those remedies are sufficiently adapted to automated contracting.

E. Relevant UNCITRAL texts

1. Electronic commerce texts

39. UNCITRAL texts on electronic commerce contain provisions dealing with various aspects of automated systems. While the provisions of these texts can be applied to AI systems, they deal only with some of the legal issues identified above, namely the validity of contracts formed and performed by automated systems.

[30] Russian Federation, Federal Law No. 34-FZ of 18 March 2019 on amendments to parts 1, 2 and article 1124 of part 3 of the Civil Code of the Russian Federation.)

40. Recalling that automated systems essentially involve the output of data messages, the MLEC contains several non-discrimination provisions that support the validity of contracts formed and performed by data messages generated by AI systems (articles 5, 11(1) and 12(1)). Specifically, it provides that neither an offer or acceptance nor the resulting contracting between the parties or a statement made by either of them are to be denied validity or enforceability on the sole ground that they are in the form of data messages (i.e. in electronic form). The MLEC also contains a rule for the attribution of data messages sent by an "information system" that is programmed to operate automatically (article 13(2)(b)). According to that rule, the data message is attributed to the person who programmed the system, or on whose behalf the system was programmed. The term "information system" is defined in the MLEC to mean a "system for generating, sending, receiving, storing or otherwise processing data messages", which would generally cover AI systems.

41. Like the MLEC, the ECC supports the validity of communications and contracts between parties in electronic form (article 8). Article 4(a) defines a "communication" to mean "any statement, declaration, demand, notice or request [...] that the parties are required to make or choose to make". Admittedly, it is conceivable that a party may seek to rely on an output of an automated system in the performance of a contract that cannot be characterized as a "communication".

42. Significantly, article 12 of the ECC contains a non-discrimination rule that expressly supports the validity of contracts formed by an "automated message system", whether by interaction with a natural person or with another such system (article 12). Specifically, the rule provides that a contract is not to be denied validity or enforceability on the sole ground that no natural person reviewed or intervened in each of the individual actions carried out by the automated message system or the resulting contract.

43. The ECC defines the term "automated message system" to mean "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 each time an action is initiated or a response is generated by the system". The explanatory note states that article 12 is based on the "paradigm that an automated message system is capable of performing only within the technical structures of its preset programming" (i.e. in a deterministic manner).[31] However, it goes on to state:

> [A]t least in theory it is conceivable that future generations of automated information systems may be created with the ability to act autonomously and not just automatically. That is, through developments in artificial intelligence, a computer

[31] *United Nations Convention on the Use of Electronic Communications in International Contracts* (United Nations publication, Sales No. E.07.V.2), para. 211.

> may be able to learn through experience, modify the instructions in its own programs and even devise new instructions.

This statement supports the view (outlined above) that an AI system can fall within the meaning of "automated message system", even though the methods or techniques used by the system were not developed at the time the ECC was concluded in 2005.[32]

2. United Nations Convention on Contracts for the International Sale of Goods

44. A preliminary issue relating to AI systems is whether an agreement to integrate an AI system into existing operations earlier in the AI lifecycle (whether for use in trade or to trade) or the supply of AI-enabled goods in trade later in the AI lifecycle involves a contract for the sale of goods to which the United Nations Convention on Contracts for the International Sale of Goods (CISG) applies. In that regard, article 3(2) of the CISG excludes from its scope "contracts in which the preponderant part of the obligations of the party who furnishes the goods consists in the supply of labour or other services". A question thus arises as to whether: (i) the contract involves the supply of services (in the case of AI-enabled goods, particularly relevant in this regard is the connectivity between the goods post-delivery and systems and data sources maintained or provided by the seller in order for the AI features of the goods to operate); and (ii) whether that supply constitutes the preponderant part of the obligation of the seller.

45. With respect to the first question, because AI is essentially software, the analysis of the supply of software under the CISG in part two of this taxonomy is relevant. With respect to the second question, case law on the CISG suggests that the application of article 3(2) requires a comparison between the economic value of the obligations relating to the supply of services and the economic value of the obligations regarding the goods, as if two separate contracts had been made.[33] Thus, if the ongoing supply of services to support the AI features of the goods amounts to more than 50 per cent of the seller's obligations, the CISG does not apply to the contract. There is also case law to suggest that a court should also take into account other factors than purely economic ones, including the circumstances surrounding the conclusion of the contract, the purpose of the contract and the interest of the parties in the various performances. In any event, article 3(2) requires a close analysis of the relevant contract on

[32] In the United States, a similar view was earlier expressed by the Uniform Law Commission in its commentary on the definition of "electronic agent" in the Uniform Electronic Transactions Act (1999), which states that, if developments in artificial intelligence occurred so as to enable autonomous capabilities, the "courts may construe the definition of electronic agent accordingly, in order to recognize such new capabilities".

[33] UNCITRAL *Digest of Case Law on the United Nations Convention on Contracts for the International Sale of Goods* (New York, 2016), p. 20.

a case-by-case basis. In that regard, services to support AI features of goods may well be supplied under a separate contract (including by a third party).

46. Another issue is whether a contract for the sale of goods that is formed using an AI or automated system is compatible with the provisions on contract formation in chapter II of the CISG. In this regard, article 11 of the CISG recognizes the principle of freedom of form for sales contracts, and thus supports their conclusion through the exchange of data messages (see also article 20(1) of the ECC) and does not appear to preclude the use of automated systems to form contracts.[34] At the same time, some provisions may not apply on their terms where AI and automated systems are used. For instance, article 14 provides that an offer is constituted by a proposal that is "addressed to one or more specific persons" provided that it is sufficiently definite and indicates "the intention of the offeror to be bound in case of acceptance". A question thus arises whether a particular AI system operates in a manner that satisfies the requirements of article 14, which in turn raises similar questions of attribution to those under general contract law (see discussion under the heading "contract formation" above).

47. Yet a further relates to the use of AI or automated systems in the performance of contracts within the scope of CISG. For instance, a question arises as to whether the remedies under the CISG for non-performance or partial-performance of the contract can be applied or are indeed sufficiently adapted. Similar questions also arise under general contract law (see discussion under the heading "contract performance" above).

48. Overall, it would appear that, while the CISG can be applied to contracts for the sale of goods that involve the use of AI systems both in trade and to trade, a range of issues relating to the applicability of its provisions are likely to arise in practice.

[34] See explanatory note to the ECC, footnote 30 above, para. 209.

Part two.

Data

A. Relevance to international trade

49. In its *Digital Economy Report 2021*,[35] UNCTAD declared that "in the digital economy, everything is data". Due to technological advances that have increased capacity to collect, transmit and analyse it, data has become a commodity in its own right. The importance of data in driving economic development has given rise to a "data economy", in which a range of data-related services are provided in a "data market". Periodic reporting by UNCTAD and the WTO point to an increasing volume of cross-border data flows and the growing value of the data market to the global economy.

50. Data is transacted along a "data value chain". It generates economic value by being transformed into "digital intelligence", which in turn becomes digital capital through its application to productive processes, such as decision-making and the development of new products.[36] Different types of data are transacted at different stages along the data value chain. While "raw data" (including "observed data" generated by sensors embedded in connected devices as part of the Internet of Things) has limited potential, "derived data" (i.e. data that is produced from raw data through processing) and "aggregated data" (i.e. a combined dataset made up of various data sources) that are produced along the data value chain have significant potential to generate value. Businesses are becoming increasingly aware of the potential of "their" data – i.e. the data that they hold and control – and of the opportunities to commercialize it in the data market.

51. Data value chains exist not only at the national level but also the international level. Cross-border data flows are particularly relevant for international trade and development and have become a common feature of digital trade agreements, including under the framework of "data free flow with trust". Significantly, efforts to regulate cross-border data flows in this context engage issues that go beyond privacy and data protection.

[35] UNCTAD, *Digital Economy Report 2021: Cross-border Data Flows and Development – For Whom the Data Flow* (Geneva, 2021), p. 4.

[36] UNCTAD, *Digital Economy Report 2019: Value Creation and Capture – Implications for Developing Countries* (Geneva, 2019), p. 29.

B. What is data?

52. According to the widely-used definition formulated by ISO, "data" is "a reinterpretable representation of information in a formalized manner, suitable for communication, interpretation or processing".[37] A similar understanding of data – as a representation of information – underlies the concept of "data message" in UNCITRAL texts on electronic commerce, which is defined as "information generated, sent, received or stored by electronic, magnetic, optical or similar means" (i.e. other than by paper-based means).[38] More recently, the recommendation adopted by the Council of the OECD in 2021 on enhancing access to and sharing of data[39] ("OECD Data Governance Recommendation") defines data in somewhat less technical terms, as "recorded information in structured or unstructured formats".

53. On the basis of the ISO definition, data need not be in electronic form or in a machine-readable format.[40] Nevertheless, it is the quality of machine-readability – and thus suitability for processing by automated systems – that gives data its value in the digital economy. For this reason, the *Principles for a Data Economy*, jointly developed by the American Law Institute and European Law Institute ("ALI/ELI Principles"), define "data" to mean "information recorded in any machine-readable format suitable for automated processing".[41] In the digital economy, machine-readable data is usually formalized in binary code consisting of a string of "zeros" and "ones". Using the language of existing UNCITRAL texts on electronic commerce, a working definition of "data" based on these definitions may be formulated in terms of a representation of information in electronic form.

54. Key to understanding how data is transacted is the concept of "processing" data. The processing of data generally refers to a range of operations that can be performed on data, including collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, transmitting, aligning or combining, and restricting, erasing or destroying.

- One or more of these operations may constitute "accessing", "sharing", "using" or "disclosing" data, which are terms that are commonly employed in international instruments, domestic legislation and contractual provisions. For instance, the OECD Data Governance Recommendation equates "data

[37] ISO, *Information Technology – Vocabulary*, ISO/IEC Standard No. 2382, 2015.

[38] MLEC, art. 2(a); ECC, art. 4(c). In the MLETR, the term "electronic record" is used.

[39] OECD, Recommendation of the Council on Enhancing Access to and Sharing of Data (2021), document C/MIN(2021)20/FINAL. The recommendation sets out general principles and policy guidance on "how governments can maximise the benefits of enhancing data access and sharing arrangements while protecting individuals' and organisations' rights and taking into account other legitimate interests and objectives".

[40] A note to the definition of "data" in ISO/IEC Standard No. 2382 states that data "can be processed by humans or by automated means".

[41] Like the ALI/ELI Principles, the principles set out in the OECD Data Governance Recommendation are "principally aimed at data in digital formats".

access" with the act of "querying or retrieving data for its potential use", while "data sharing" is the act of "providing data access for use by others".

- "Transmitting" or "sharing" data for processing in another jurisdiction may involve the cross-border "flow" of that data.
- One or more of the operations may evidence the "holding" or "control" of data, and may result in the "generation" of new data (i.e. "derived data").

55. As indicated above (section A), data can be characterized as "raw" (unprocessed) or "derived" (produced by processing other data). Data can also be categorized by reference to (i) the person who controls the data (e.g., public data, private data), (ii) the person to whom the data relates (e.g., personal data[42]), (iii) the content of the data (e.g., proprietary data,[43] corporate data, technical data), (iv) the purpose for generating the data,[44] or (v) the format of the data (e.g., structured data, unstructured data). In the case of personal data, it can be further categorized by reference to the method by which it is collected or generated (e.g., "volunteered" data provided by the data subject, "observed" data generated by interactions with the data subject). These categories, which often overlap, indicate that transactions in data can engage a wide range of actors and a wide range of laws (as elaborated below).

56. By focusing on data as a representation of "information", the working definition allows certain types of data to be distinguished, including software (i.e. data comprising computer code) and digital assets (i.e. data comprising an electronic record that is capable of being controlled and uniquely identified, as defined in part three of this taxonomy). Transactions in software and digital assets are not concerned with data as a representation of "information" – in the sense of material that can be given meaning in a particular context – but rather with data as the means to effect processes that give software and digital assets their value. For that reason, the ALI/ELI Principles expressly exclude "functional data" (defined as "data the main purpose of which is to deliver particular functionalities") and "representative data" (defined as "data the main purpose of which is to represent other assets or value") as a means to exclude from scope transactions in software and digital assets, respectively.[45] In the case of digital assets, the UK Jurisdiction Taskforce[46] has explained that "it is not what the data [representing a digital asset] tells you but what it allows you to do".[47] Similar explanations have been offered in legal doctrine to distinguish software.

[42] The term "personal data" is widely used to refer to data relating to an identified or identifiable natural person.

[43] The concept of "proprietary data" is understood as data that is subject to "data rights" as described in section D below, in particular the protections afforded under laws relating to trade secrets, copyright and database rights.

[44] This is used by the World Bank to distinguish "public intent data" and "private intent data": *World Development Report 2021: Data for Better Lives* (Washington, 2021).

[45] ALI/ELI Principles, principle 2(1).

[46] The UK Jurisdiction Taskforce is a taskforce of the "LawtechUK Panel" that was established by the Government of the United Kingdom, the judiciary of England and Wales, and the Law Society of England and Wales.

[47] "Legal Statement on Cryptoassets and Smart Contracts", November 2019, para. 60.

C. Actors

57. The data value chain involves not only a range of different stages in the processing of data but also a range of different actors. These actors may be defined by the (potentially overlapping) roles that they perform along the data value chain, and include:

- *Data generator* – the person who generates data, including by way of a machine or sensor.
- *Data subject* – the person to whom data relates, whether a legal person or natural person.
- *Data provider* – the person who provides data to another person. Depending on the transaction, the data provider may be the data generator, data subject or data controller.
- *Data recipient* – the person who receives data from another person, including by gaining access to the data shared on an online platform (for data transactions on online platforms, see part four of this taxonomy). Depending on the transaction, the data recipient may be the data processor or data controller.
- *Data controller* – the person who "holds" data or "controls" how it is processed.
- *Data processor* – the person who processes data, which encompasses almost all other roles, but often refers to persons in contradistinction to the data controller. The data processor may be a platform operator.

58. The interaction between the various actors and roles that they perform is sometimes referred to as the "data ecosystem".

D. Legal regimes

59. In the trade context, data is generally transacted between actors under contract ("data contracts"). Contract law, including the terms of the contract itself, will therefore be a primary source of the legal rights and obligations of the parties to the data transaction. However, not all actors along the data value chain will be in a contractual relationship with one another, and may therefore need to rely on other legal regimes to protect their interests in the data being processed.

1. Contract law

60. Data contracts can be categorized by reference to the role played by each of the parties to the contract. Specifically, a rough distinction can be drawn between contracts for the provision of data and contracts for the processing of data.

- *Data provision contract* – this type of data contract involves a party (the "data provider") providing data to another party (the "data recipient") for the other party to process for their own purposes. The data provider may provide the data by "sharing" the data with the data recipient or by giving the data recipient "access" to the data. As recognized by the OECD Data Governance Recommendation, "sharing" and "accessing" are therefore opposite sides of the data transaction. This may be done in many ways, including by causing the data to be stored in an online space hosted by a third-party platform operator that is accessible by the data recipient, or by giving the data recipient access to a data source that the data provider controls.
- *Data processing contract* – this type of data contract involves a party (the "service provider") processing data for another party (the "service recipient") and providing the processed data to the other party. Common types of data processing transactions include data scraping, cloud-based services, data analytics, data pooling and electronic transmission services. While data processing contracts involve the provision of data between the parties (e.g., data provided by the service recipient to be processed and the resulting processed data provided by the service provider), they are predominantly concerned with the provision of services.

61. Several national and international initiatives have sought to categorize the rights and obligations under data contracts (using slightly different typologies).

- The ALI/ELI Principles identify different types of data contracts under the categories of "contracts for supply or sharing of data" and "contracts for services with regard to data". For each type of contract, the ALI/ELI Principles specify a set of default terms governing the contractual relations of the parties with respect to the relevant data transaction.
- In 2018, the Ministry of Economy, Trade and Industry of Japan published contract guidelines on the utilization of data (hereafter the "METI Data Guidelines")[48] with a view to "promoting reasonable negotiations and execution of contracts, reducing transaction costs and diffusing data contracts". The METI Data Guidelines specify distinguish three types of data contracts – data provision contracts, data generation contracts and data sharing contracts using platforms – and provide commentary on a range of issues that the parties are advised to address in each type of contract.
- In 2023, the Ministry of Trade, Industry and Energy of the Republic of Korea published contract guidelines on industrial data. The guidelines describe the main issues associated with three types of data contracts – data provision contracts, data generation contract, and data sharing contracts (using a platform).

[48] Japan, Ministry of Economy, Trade and Industry, *Contract Guidelines on Utilization of AI and Data: Data Section* (June 2018), p. 1.

62. Data provision contracts will generally contain terms addressing the following data-specific issues:

- *What the data is* – description of the types of data to be provided under the contract.
- *How the data is provided* – if data is transferred to a medium (e.g. a disk, a server or an online platform), which party has control of the medium; if access is given to data or to a data source, whether the data provider merely provides access or does more to facilitate that access.
- *Conformity of the data* – description and warranties as to the quantity and quality of the data, including in terms of its completeness, accuracy and format, as well as conformity with any relevant industry or international standards or representations made by the data provider.
- *Use of the data by the data recipient* – description and warranties as to how the data recipient may use (or more generally process) the data, including any limitations on use by reference to purpose, third party rights or use by the data provider.
- *Use of the data by the data provider* – description of how the data provider may use the data (if at all), as well as any use of any new data generated by the data recipient in its use of the data.
- *Dealing with data upon breach or avoidance* – description of how the defaulting party is to deal with the data in the event of breach or avoidance of the contract.

63. Data processing contracts will generally contain terms addressing the following data-specific issues:

- *Scope and purpose of services* – description of the data processing services provided by the service provider.
- *Data security and data integrity* – description of the policies and procedures for maintaining data security and integrity, and for managing security incidents.
- *Data portability* – description of processes available to the service recipient to access data in a format that is usable in systems other that the system provided by the service provider.
- *Data localization* – any limitations on the locations in which the data is processed.
- *Use of the data by the service provider* – description of how the service provider may use data collected under the contract, particularly data collected from the service recipient, and data provided under the contract, including any limitations on use and obligations to deliver up data at the end of the contract term.

64. Beyond their terms, data contracts are subject to the general principles of contract law that are designed to ensure good faith and fair dealing, as well as rules that are designed to fill gaps in the contract to give effect to the underlying transaction. The application of these rules generally requires an analysis of the nature and purpose of the contract and established commercial practice, which in the context of data contracts calls for an understanding of the data economy. The initiatives mentioned above point to a degree of uncertainty among actors about negotiating the terms of data contracts, as well as the application of general principles of contract law to these contracts. For instance, the introductory note to the ALI/ELI Principles makes the following observation.

> Both in the United States and in Europe, uncertainty as to the applicable rules and doctrines to govern the data economy is beginning to trouble stakeholders (such as data-driven industries, micro, small and medium-sized enterprises, as well as consumers). This uncertainty undermines the predictability necessary for efficient transactions in data, may inhibit innovation and growth, and may lead to market failure and manifest unfairness, in particular for the weaker party in a commercial relationship.

2. Property law

65. While it is common to refer to data as "belonging" to someone (e.g. the data subject or the data controller), data is generally not recognized in law as an object of property rights, and thus not amenable to "ownership" and the rights attributed to ownership under law (e.g. the right to use and to control). In civil law jurisdictions, data is generally not listed as an object of property rights in the civil code, which generally confines such objects to tangible things. In common law jurisdictions, it has been observed that "the law has been reluctant to treat information itself as property".[49] In England, for instance, the Court of Appeal confirmed in a 2014 judgment that data in an electronic database is not tangible property for the purposes of English common law and therefore that: (i) data is not capable of being the subject of a possessory lien (i.e. the right of a bailee to refuse to return property); and (ii) withholding data cannot be the subject of a claim for conversion (i.e. a claim for the wrongful interference with property).[50]

66. Legal doctrine tends to support the status quo, not only in view of the "non-rivalrous" nature of data (in the sense that the use of data by one person does not limit its use by another person due to the ease with which data can be replicated), but also

[49] *Your Response v. Datateam Business Media,* Case No. B2/2013/1812, Judgment, 14 March 2014, *Official Law Reports: Queen's Bench Division*, vol. 2015, p. 41, [2014] EWCA Civ 281, para. 42 (Lord Justice Floyd). For a list of cases confirming this position in Australia, Canada, the United Kingdom and the United States, see Court of Appeal of England and Wales, *Thaler v. Comptroller General of Patents Trade Marks and Designs*, Case No. A3/2020/1851, Judgment, 21 September 2021, [2021] EWCA Civ 1374, para. 125 (Lord Justice Arnold).

[50] Ibid.

out of concern that vesting property rights in data could ultimately harm data flows, limit business opportunities in the data economy, and undermine the overall integrity of the existing property law regime. Moreover, in a 2018 communication on establishing a common data space in the European Union, the European Commission reported that, as regards business-to-business data sharing, stakeholders "do not favour a new 'data ownership' type of right", on the basis that "the crucial question in business-to-business sharing is not so much about ownership, but about how access is organized".[51]

67. Nevertheless, the law in some jurisdictions has moved to recognize certain data products (i.e., products comprised of data) as objects of property rights (for a discussion of digital assets, see part three of this taxonomy).

- In Germany, where the courts have confirmed that data is not a "thing" under section 90 of the Civil Code, the 2021 Electronic Securities Act specifically provides that "crypto securities" within the meaning of that law are "things" for the purposes of the Civil Code.
- In China, article 127 of the Civil Code (and the General Provisions of the Civil Law before it) signals that "online virtual assets" may be protected by law, but does not expressly recognize such assets as an object of property rights, nor define them. In a 2018 judgment, a first instance court in Zhejiang province recognized rights and interests in big data products claimed by a network operator from the perspective of competition law in order to protect the network operator's investment in such products. However, in the absence of any existing legislation dealing with rights over data products, the court refused to recognize ownership over the data products, noting that ownership was an absolute right and, if granted to network operators, corresponding obligations would be imposed on an unspecified majority of the population.[52] This finding was confirmed in 2019 by the Zhejiang Higher People's Court, which described the rights and interests in the data products as "competitive property rights and interests".[53]
- In England, the Court of Appeal conceded in the case of *Your Response v. Datateam Business Media* that there was a "powerful case" for recognizing "digitized materials" as a new category of property, but added that this legal development would require "the intervention of Parliament".[54]
- In New Zealand, the courts have shown a willingness to extend the categories of property at common law into the digital realm without legislative intervention. In a 2019 judgment in the case of *Henderson v. Walker*, the

[51] Document COM(2018) 232 final 9.

[52] Hangzhou Railway Transportation Court (now the Hangzhou Internet Court), *Taobao (China) Software Co., Ltd. v. Anhui Meijing Information Technology Co., Ltd.*, Zhe 8601 Min Chu No. 4034, Judgment, 16 August 2018.

[53] Zhejiang High People's Court, *Anhui Meijing Information Technology Co., Ltd. v. Taobao (China) Software Co., Ltd.*, Zhe Min Shen No. 1209, Judgment, 2 July 2019.

[54] See footnote 49 above, para. 27.

High Court of New Zealand held that digital files stored on a computer were capable of possession and therefore that interference with those files could give rise to a claim for conversion.[55] The court stated that this applied to all "digital assets", which it defined to include "all forms of information stored digitally on an electronic device, such as emails, digital files, digital footage and computer programmes" (note that these are not the same types of digital assets that are the focus of part three of this taxonomy).[56]

- In the United States, it has been accepted in some states that a claim for conversion can extend to intangible objects.[57] For instance, in the case of *Thyroff v. Nationwide Mutual Insurance Co.*, the Court of Appeals of the state of New York held that a claim for conversion under the law of that state extended to "electronic records that were stored on a computer and were indistinguishable from printed documents", which in that case comprised customer and personal information stored in a principal's computer system accessible by an agent through a licensed computer.[58] The court nevertheless cautioned that it did not consider "whether any of the myriad other forms of virtual information should be protected by the tort".[59]
- In the European Union, some legal commentators regard the judgment of the Court of Justice in the *UsedSoft* case as opening up a discussion on ownership of data products.[60] In that case, the court held that the commercial distribution of software by Internet download could constitute a "sale" for the purposes of Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the Legal Protection of Computer Programs. In reaching that conclusion, the court held that, according to a commonly accepted definition, a "sale" was an agreement by which "rights of ownership in an item of tangible or intangible property belonging to [one person]" are transferred to another person in return for payment, and reasoned that a "commercial transaction giving rise … to exhaustion of the right of distribution of a copy of a computer program must involve a

[55] *Henderson v. Walker*, Case No. CIV2014-409-45, Judgment, 3 September 2019, *New Zealand Law Reports*, vol. 2021, No. 2, p. 630, [2019] NZHC 2184.

[56] Ibid, para. 263. It is not clear whether this case represents authority that *all* data, regardless of its format, would be protected by a claim for conversion. While the High Court emphasized that there was a "real difference between digital assets and the information they record", the High Court stated in a subsequent case that the decision in *Henderson v. Walker* extends the claim for conversion "to purely digital information": *Ruscoe v. Cryptopia Limited (in liquidation)*, Case No. CIV2019-409-000544, Judgment, 8 April 2020, *New Zealand Law Reports*, vol. 2020, No. 2, p. 809, [2020] NZHC 728, para. 91.

[57] *Kremen v. Cohen.*, Case No. 0115899, Judgment, 25 July 2003, *Federal Reporter, Third Series*, vol. 337, p. 1024, [2003] USCA9 49.

[58] *Thyroff v. Nationwide Mutual Insurance Co.*, Judgment, 22 March 2007, *New York Reports, Third Series*, vol. 8, pp. 292–3.

[59] Ibid., p. 293.

[60] *UsedSoft GmbH v. Oracle International Corporation*, Case No. C-128/11, Judgment, 3 July 2012.

transfer of the right of ownership in that copy".[61] The implications of the judgment for data products beyond software transactions and for other areas of European Union law remain to be seen.

3. Other laws

Laws relating to data transactions

68. As between the parties to a data transaction, contract law is supplemented by specific legislation regarding contracts for the sale of goods. While data provision is sometimes likened to the "sale" of data, data transactions are usually not covered by this legislation because (i) the concept of "goods" is limited to tangible things, or (ii) the concept of a "sale" is tied to the transfer of ownership, and thus to transactions involving objects that are the subject of property rights. In some jurisdictions, legislative reform and case law have extended sale of goods laws to apply to software transactions.[62] Suggestions have been made in legal doctrine that sale of goods law should be applied to data transactions more generally.

69. In the European Union, a series of regulations have been introduced or proposed to regulate data transactions. For instance, a framework regulation for the free flow of non-personal data (i.e., data other than "personal data") was adopted in 2018[63] with a particular focus on cloud service providers. Among other things, the regulation provides for the development of industry codes of conduct for data portability to avoid so-called "vendor lock-in practices" and to encourage competition in the data market. More recently, the European Commission has submitted proposals to regulate other types of data processing transactions, as well as to prohibit certain unfair terms in data provision contracts with MSMEs on data-specific matters such as the assessment of conformity and limitations on access and use.

70. Data transactions are also subject to laws in many jurisdictions that restrict cross-border data flows. These laws include privacy and data protection laws, national security laws, laws designed to ensure that authorities have access to information to perform regulatory oversight and laws designed to help develop domestic capacity in digitally intensive sectors.[64]

[61] Ibid., para. 42.

[62] In the United States, the Uniform Law Commission has prepared a model law – the Uniform Computer Information Transactions Act (2002) – to regulate transactions in computer information products such as computer software and online databases, although the model law has not been widely enacted in individual states of the United States.

[63] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a Framework for the Free Flow of Non-Personal Data in the European Union.

[64] Francesca Casalini and Javier López González, "Trade and Cross-Border Data Flows", *OECD Trade Policy Papers*, No. 220 (Paris, 23 January 2019), p. 5.

Laws relating to data rights

71. A variety of other legal regimes provide additional "layers" of protection with respect to certain types of data or data products, including laws on copyright, database rights, privacy and data protection, trade secrets and confidential information. While these regimes pursue different policy objectives, they all afford varying degrees of control over how data is processed by establishing rights, claims and remedies against third party processing. This control includes (i) gaining access to data held by the third party, (ii) requiring the third party to desist from processing data and (iii) requiring the third party to correct or erase the data. These controls are referred to in this taxonomy as "data rights", although the term – as with the term "data transactions" itself – is not yet firmly established in legislation or legal doctrine.

72. Data rights established under these legal regimes generally apply with mandatory effect and are therefore independent of any data contract. Nevertheless, data rights and data contracts do intersect. For instance, similar rights as between the parties to a data transaction may be established in the data contract. Moreover, the data contract may contain warranties by either party as to the compliance of the data or its use or processing under the contract with the data rights of a third party. While sometimes characterized as "property" or "property-like", data rights are independent of existing property law regimes.

73. Legislation has been introduced in several jurisdictions to establish additional data rights. Moreover, a number of national and international law reform initiatives have proposed data rights.

- In some jurisdictions, the law establishes a right to data held by a third party in the event of insolvency[65] or a right to access certain data held by a third party in the event of death or incapacity.[66]
- In Japan, the Unfair Competition Prevention Act was amended in 2018 to introduce provisions on unfair competition related to data with a view to promoting a business environment that "rewards the efforts of data creators, collectors, analysers, and controllers".[67] The provisions apply to "shared data with limited access", which is defined to comprise technical or business data that is provided by the data holder to specified persons on a regular basis, for example market analysis data, operational data and data relevant to an ongoing business relationship (e.g.,

[65] Luxembourg, Law of 9 July 2013 modifying article 567 of the Commercial Code, *Official Gazette of the Grand Duchy of Luxembourg*, vol. 2577, No. 124 (18 July 2013), p. 2578.

[66] In the United States, the Uniform Law Commission has prepared the Revised Uniform Fiduciary Access to Digital Assets Act (2015), which has been enacted in almost all states of the United States. Similar model laws have been prepared in Canada and proposed for other jurisdictions.

[67] See Ministry of Economy, Trade and Industry, *Guidelines on Shared Data with Limited Access* (23 January 2019), pp. 3–5.

under a franchise or joint venture arrangement). As amended, the Unfair Competition Prevention Act prescribes a range of acts related to such data, which can broadly be divided into three categories, namely: (i) wrongful acquisition from the data holder; (ii) use or disclosure in circumstances constituting a significant breach of good faith toward the data holder; and (iii) subsequent acquisition or disclosure of data with knowledge of its wrongful acquisition or improper disclosure. Existing civil remedies under the Unfair Competition Prevention Act, including injunctions and claims for damages, are available to the data holder. With the exception of the second category, unfair competition related to "shared data with limited access" does not presuppose the existence of a contractual relationship between the data holder and the wrongdoer.

- In the Republic of Korea, the Unfair Competition Prevention and Trade Secret Protection Act was amended in 2021 to clarify how the unfair competition regime applies to data that is provided in the course of business, in particular data that is not otherwise subject to protections related to trade secrets, copyright and database rights. As amended, the Act defines each of the following as an "act of unfair competition": (i) unauthorized acquisition and use of data; (ii) use of data in circumstances constituting a breach of good faith; and (iii) the subsequent acquisition of data with knowledge of its unauthorized acquisition. Among other things, an act of unfair competition with respect to data is subject to civil remedies under the Act, including injunctions and claims for damages.

- In India, a committee of experts commissioned by the Government to deliberate on a non-personal data governance framework released a report in 2020 that explores mechanisms to establish rights over non-personal data. In particular, the report examines the possibility of conferring on a "community" – defined as "any group of people that are bound by common interests and purposes, and involved in social and/or economic interactions" – the right to derive economic and other value from data produced by the community, and the right to eliminate or minimize harms to the community.[68]

- The ALI/ELI Principles recognize a number of rights regarding the downstream processing of data. For instance, the ALI/ELI Principles recognize rights in "co-generated data" pursuant to the principle that "whoever has contributed to the generation of data should generally have some rights with respect to its use or with respect to the value it generates".[69] The content of these rights depends on the circumstances surrounding the generation of data, and may include accessing the data, requiring a data

[68] Ministry of Electronics and Information Technology, *Report by the Committee of Experts on Non-Personal Data Governance Framework* (16 December 2020), ch. 7.

[69] ALI/ELI Principles, p. 28.

controller to desist from processing the data, or to correct or erase the data, or, in exceptional circumstances, claiming an economic share in profits derived by the data controller from the use of the data.

4. Private international law

74. Cross-border data flows raise private international law issues. In particular, the special nature of data, which can be stored and processed in multiple locations, may present challenges to the application of choice of law rules.

E. Relevant UNCITRAL texts

1. United Nations Convention on Contracts for the International Sale of Goods

75. The CISG applies to "contracts of sale of goods" (article 1(1)). Whether it applies to data transactions has evoked a lively debate in legal doctrine regarding software transactions, which centres on two issues: first, whether software can be characterized as "goods" (a term that is not defined in the CISG), and second, whether the provision of software under contract can be characterized as a "contract of sale".

- On the first issue, the UNCITRAL secretariat has observed that the CISG "seems to embody a rather conservative concept of 'goods', as it is considered both in legal writings and case law to apply basically to moveable tangible goods".[70] On that basis, while a data storage device would be characterized as "goods", the data itself would not.
- On the second issue, the UNCITRAL secretariat has observed that, while the term "contract of sale" is not defined in the CISG, its meaning can be determined by reference to its context, specifically the rights and obligations of the parties to the contract of sale provided under the CISG. Thus, the contract of sale involves the delivery of goods and transfer of property, and can thus be distinguished from a licence agreement.[71] Given that the supply of software involves the copying of data (i.e. the computer code) and does not involve the "transfer" of data, the supply can only be characterized as a licence and not a "sale". Admittedly, there have been cases in which courts have characterized a software transaction as a "sale" for the purposes of the CISG.[72] However, data transactions present an additional difficulty given

[70] A/CN.9/WG.IV/WP.91, para. 21.

[71] Ibid., paras. 27–28.

[72] See, e.g., Midden-Nederland District Court, *Corporate Web Solutions v. Dutch company and Vendorlink B.V.*, Case No. C/16/364668, Judgment, 25 March 2015. Abstract published in A/CN.9/SER.C/ABSTRACTS/170, p. 11.

that data is generally not recognized in law as an object of property rights (see subsection D.2 above).

76. Nevertheless, it has been suggested in legal doctrine that the CISG could serve as a blueprint for regulating data transactions. For data processing contracts, an additional question arises as to whether the provision of the service constitutes the "preponderant part" of the contract, thereby triggering the exclusion in article 3(2) CISG.

2. Electronic commerce texts

77. UNCITRAL electronic commerce texts give legal recognition to data comprising the electronic communications and records and that are used by commercial parties in the course of business. Specifically, the MLEC provides that an offer and acceptance may be expressed by means of data messages, and that neither a contract nor any statement between the contracting parties shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose (articles 11(1) and 12(1)). A similar provision is found in the ECC (article 8(1)). Moreover, the MLETR provides that an electronic transferable record satisfying the conditions of the model law shall not be denied legal effect, validity or enforceability on the sole ground that it is in electronic form (article 10).

78. It is also worth mentioning article 6 of the ECC and article 14 of the MLETR, which reflect the principle that the location of communications technology and equipment is of limited value in determining the location of a person's place of business. This principle is particularly relevant to data, where the question of the location of the parties to a data transaction or the location of data processing may arise in the application of other laws.

3. Notes on the Main Issues of Cloud Computing Contracts

79. As indicated above (subsection D.1), cloud-based services are a form of data processing. The Notes on the Main Issues of Cloud Computing Contracts, prepared by the secretariat and approved for publication by the Commission in 2019, contain a non-exhaustive analysis of issues for consideration by parties before and during the drafting of contracts for cloud-based services, including the application of mandatory laws and the issues to be addressed in the contract.

80. While not prepared with data transactions in mind, the issues analysed in the text are relevant to the conclusion of data processing contracts, including the data-specific issues usually contained in those contracts (as listed in subsection D.1 above).

Part three.

Digital assets

A. Relevance to international trade

81. The digital economy is witnessing a shift in how economic value is held. Digital assets are playing an increasingly important role in trade, where they are used as items of trade and objects of trade-related services, a method of payment, collateral for raising finance, an investment vehicle, a consumable in business operations, and a tool for improving business processes. Digital assets have the potential to leverage emerging technologies and applications to deliver a range of benefits to business, including efficiency gains driven by automation and disintermediation, greater transparency, faster and potentially more efficient clearing and settlement, lower barriers to investment, and enhanced access to finance for MSMEs.[73]

B. What is a digital asset?

82. There is no widely accepted definition of a digital asset, for which various different names exist.[74] In its ordinary meaning, the term "digital asset" connotes a collection of data, stored electronically, that is of use or value. For instance, in the context of DLT systems, the ISO defines a "digital asset" as an asset, i.e. "anything that has value to a stakeholder", that "exists only in digital form or which is the digital representation of another asset".[75] A similar meaning is given in legislation enacted in some jurisdictions to provide fiduciaries with access to "digital assets" in the event of death or incapacity.

- In Canada, the Uniform Access to Digital Assets by Fiduciaries Act prepared by the Uniform Law Conference[76] defines "digital asset" to mean "a record that is created, recorded, transmitted or stored in digital or other intangible form by electronic, magnetic or optical means or by any other

[73] OECD, *The Tokenization of Assets and Potential Implications for Financial Markets*, OECD Blockchain Series, 2020, pp. 7, 16–17.

[74] Digital assets are sometimes referred to as "cryptoassets" in reference to the cryptographic techniques used to authenticate transactions involving the digital asset. They are sometimes also referred to as "tokens".

[75] ISO, *Blockchain and Distributed Ledger Technologies – Vocabulary*, ISO Standard No. 22739, 2020.

[76] Uniform Law Conference of Canada, Uniform Access to Digital Assets by Fiduciaries Act (2016).

similar means".[77] The commentary on the definition explains that the term covers: (i) any information stored on a computer and other digital devices; (ii) content uploaded onto websites, ranging from photos to documents; and (iii) rights in digital property, such as domain names or digital entitlements associated with online games and material created online.

- In the United States, the Revised Uniform Fiduciary Access to Digital Assets Act (2015), prepared by the Uniform Law Commission and enacted in almost all states of the United States, defines "digital asset" to mean "an electronic record in which an individual has a right or interest".[78] The commentary states that digital assets within the meaning of the uniform law "rang[e] from online gaming items to photos, to digital music, to client lists" and "can have real economic or sentimental value".[79]

83. If the term "digital asset" is given its ordinary meaning, the concept is already well known to UNCITRAL texts on electronic commerce. In this sense, a digital asset is essentially a collection of "data messages" within the meaning of the MLEC or an "electronic record" within the meaning of the MLETR.

84. However, certain types of digital assets (within the ordinary meaning of the term) have been singled out as having particular economic value, and thus relevance to trade.

- *Cryptocurrencies* – Digital assets that represent intrinsic value owing to the rules of the system in which the data constituting or representing the digital asset is stored or processed. When used as a means of payment, these digital assets are sometimes referred to as "payment" tokens, the most common form of which are cryptocurrencies; and

- *Asset-backed digital tokens* – Digital assets that represent value owing to a link between the digital asset and some "real world" tangible or intangible asset, such as goods or digital products (or rights therein), receivables (i.e., rights to payment) and other claims. The link is established by the rules of the system in which the data constituting or representing the digital asset is stored or processed. The linked asset may be referred to as a "tokenized" asset by reference to the creation of a digital "token" to which it is linked; thus, the process of issuing such tokens is referred to as the "tokenization" of assets[80] and the tokens issued are referred to as "asset-backed". A common form of

[77] This definition picks up the definition of "electronic" in the Uniform Electronic Commerce Act adopted by the ULCC.

[78] Revised Uniform Fiduciary Access to Digital Assets Act (2015) with Prefatory Note and Comments.

[79] The commentary explains that the "right or interest" that the individual has in the electronic records must be a "property right or interest". If, unlike the Canadian uniform law, the subsistence of a property right or interest is a defining feature of a digital asset, the definition would appear to avoid the question as to whether digital assets are an object of property rights (discussed below).

[80] See OECD, footnote 73.

digital asset in this sense is what is sometimes referred to as a "security" or "investment" token, which purports to represent a right to share in the profits of a particular enterprise. Other forms include "utility" tokens, which purport to represent rights to use a service provided on the platform that supports the token, "governance" tokens, which purport to represent rights to vote in a governance framework, and "non-fungible" tokens (or "NFTs"), which are linked to goods or other digital products that are purported to be unique or identifiable.

85. In the trade context, it has been suggested that the feature of legal significance that distinguishes these types of digital assets – i.e. cryptocurrencies and asset-backed digital tokens – from a mere collection of data messages or an electronic record is their transferability. This in turn presupposes that the digital asset is supported by a system that provides control over the asset, in the sense that the asset is capable of being controlled (which control may be transferred from one person to another). It also presupposes that the system provides some guarantee as to the singularity or rivalrousness of the digital asset, in the sense that the digital asset can be singled out and secured against replication. Several legislative initiatives have identified controllability, singularity and rivalrousness as defining features of digital assets.

- The 2023 UNIDROIT Principles on Digital Assets and Private Law provide legislative guidance on digital assets that are used in trade. The Principles define a digital asset as an electronic record which is capable of being subject to exclusive control.
- Controllability and singularity are the defining features of an "electronic transferable record" under the MLETR, which is a particular type of digital asset.[81]

86. Digital assets with these features can be supported by a variety of technologies and methods. For instance, they can exist in centralized systems (e.g., centralized registries of dematerialized securities or a gaming platform supporting virtual payment tokens). In this form, digital assets are not a new phenomenon. More recently, the uptake of distributed ledger technology (explored in part five of this taxonomy) has allowed such digital assets to exist in decentralized systems.

[81] See art. 10(1) of the MLETR, which provides that an electronic transferable record meets the requirement of a paper-based transferable document or instrument if, among other things, a reliable method is used: (i) to identify that electronic record as the electronic transferable record; (ii) to render that electronic record capable of being subject to control from its creation until it ceases to have any effect or validity; and (iii) to retain the integrity of that electronic record. See also art. 17(3) of the MLEC, which establishes a "guarantee of singularity" to permit the use of electronic transport documents: *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with Additional Article 5* bis *as Adopted in 1998* (United Nations publication, Sales No. E.99.V.4), para. 115.

87. Several jurisdictions have introduced legislation that defines tradeable digital assets. While much of this legislation deals with regulatory aspects,[82] some legislation deals with private law aspects of digital assets.

- In Belarus, Presidential Decree No 8 of 2017 on the development of the digital economy confers on the residents of the Minsk Hi-Tech Park the right to possess "tokens", which are defined to mean "a record in transaction block ledger (blockchain)… which verifies that the owner of a digital sign (token) has rights to civil-law objects and/or is cryptocurrency".[83]
- In Bermuda, the Digital Asset Business Act 2018 was enacted to regulate "digital asset business activities", including the issuance and sale of digital assets and the operation of exchanges for trading digital assets for fiat currency or bank credit. The legislation defines "digital asset" as "anything that exists in binary format and comes with the right to use it". The legislation includes within the definition any digital representation of value that (i) is used as money, (ii) is intended to represent an asset or right associated with an asset, or (iii) is intended to provide access to an application or service or product by means of distributed ledger technology. It expressly excludes from the definition (i) loyalty points that cannot be redeemed for legal tender, bank credit or other digital assets, and (ii) gaming tokens.[84]
- In Liechtenstein, a law was enacted in 2019 to establish a legal framework for transacting in digital tokens.[85] The law defines "token" as a piece of information on a transaction system using "trustworthy technology" that "can represent claims or rights of membership against a person, rights to property or other absolute or relative rights". The law is based on a "container" model whereby tokens are likened to containers that are "loaded" with rights. While the definition is primarily focused on asset-backed digital tokens, the law is also relevant to cryptocurrencies, which are likened to tokens that are "empty" containers. The law refers to the transaction system in technology-neutral terms, using the term "trustworthy technology" to mean "technologies through which the integrity of tokens, the

[82] See, e.g., France, Law No. 2019-486 of 22 May 2019 on Business Growth and Transformation, which amends the Monetary and Financial Code to establish a regulatory regime for digital asset service providers. Article L. 54-10-1 of the amended Code defines digital asset to mean (i) tokens other than those constituting financial securities and (ii) cryptocurrency. Article L. 552-2 in turn defines a "token" as "any intangible property representing, in digital form, one or more rights that may be registered, retained or transferred by means of a shared electronic recording device that identifies, directly or indirectly, the owner of such property".

[83] Decree of the President of the Republic of Belarus No. 8 of 21 December 2017 on Development of Digital Economy, annex 1, cl. 12.

[84] Bermuda, *Digital Asset Business Act*, sect. 2(1).

[85] Liechtenstein, Law of 3 October 2019 on Tokens and TT Service Providers, *Liechtensteinisches Landesgesetzblatt*, vol. 2019, No. 301 (2 December 2019).

clear assignment of tokens… and the disposal over tokens is ensured". No reference is made in the law to distributed ledger technology.[86]

- In the United States, a Digital Assets Act was introduced in the state of Wyoming[87] in 2019 for the purposes of bringing digital assets under the state's secured transactions law.[88] The Digital Assets Act defines a digital asset as "a representation of economic, proprietary or access rights that is stored in a computer readable format, and includes digital consumer assets, digital securities and virtual currency".[89]

88. Using the language of existing UNCITRAL texts on electronic commerce, and in keeping with the principle of technology neutrality, a working definition of "digital asset" based on these definitions may be formulated in terms of an electronic record (i.e. a data message or collection of data messages that are logically associated or otherwise linked together) that is capable of being controlled and uniquely identified.

C. Actors

89. The use of digital assets generally involves the following actors:

- *Administrator* – the person who administers the system that supports the digital asset.
- *Holder* – the person who holds the digital asset.
- *Beneficiary* – any person on whose behalf the digital asset is held (e.g., if the digital asset is held by an intermediary such as a cryptocurrency exchange or "wallet" service provider in the case of DLT-based digital assets).
- *Counterparty* – if the digital asset is in the form of an asset-backed digital token, the person against whom the rights represented by the token may be asserted (e.g., the person who issued the token).

[86] As the report of the Government on the proposed law notes, "[t]o prevent this Law from becoming outdated from a technical perspective and having a limited scope of application in just a few years, the technologyneutral formulation of the term "blockchain" is very important": *Report and Application of the Government to the Parliament of the Principality of Liechtenstein concerning the Creation of a Law on Tokens and TT Service Providers (Tokens and TT Service Provider Act; TVTG) and the Amendment of Other Laws*, No. 54/2019, 7 May 2019, para. 52.

[87] United States, *Wyoming Statutes*, Title 34, Chap. 29, sect. 101(a)(i).

[88] Uniform Commercial Code, art. 9, as adopted in Wyoming: *Wyoming Statutes*, Title 34.1.

[89] United States, *Wyoming Statutes*, Title 34, Chap. 29, sect. 101(a)(i).

D. Legal regimes

1. Contract law

90. The rules of the system determine how the digital asset is created and transferred. These rules are encoded in the software that runs the system and may be put on a contractual footing by agreement between the administrator and the person holding the digital asset. In decentralized systems that run on open-source software, the only contract may be the end-user agreement to use the software (the governance of DLT systems is explored further in part five of this taxonomy). In other systems, including centralized systems, the contract may be more prescriptive on matters relating to the administration of the system (the governance of online platforms is explored in part four of this taxonomy).

91. The transfer of a digital asset will generally be done under a contract. Similarly, any dealings in the linked asset will generally be done under a contract (e.g., a sales agreement or security agreement). There may also be a contract between the person who holds the digital asset and the person on whose behalf the digital asset is held (e.g., a custodian agreement).

2. Property law

(a) Digital assets in the form of cryptocurrency

92. One of the key legal questions surrounding digital assets, particularly those in the form of cryptocurrency, is whether they constitute an object of property rights. To the extent that they are merely comprised of data, digital assets, like data, are generally not recognized in law as an object of property rights. As noted in part two of this taxonomy, the civil codes of many civil law jurisdictions only establish property rights in tangible "things". Nevertheless, the law in some civil law jurisdictions has moved to recognize certain digital assets as object of property.

- In Japan, pursuant to article 85 of the Civil Code, the property law regime under chapter IV of the Civil Code only applies in relation to tangible things. In a 2015 decision, the Tokyo District Court confirmed that Bitcoin could not be classified as a "thing" for the purposes of the Civil Code.[90]
- In Liechtenstein, when preparing the 2019 law to establish a legal framework for transacting in digital tokens, the Government considered whether the law should be amended to recognize tokens as an object of property rights. To explain the decision not to do so, the Government stated that

[90] Tokyo District Court, *Plaintiff Z1 v. Mt. Gox Co. Ltd.*, Case No. 2014 (Wa) 33320, Judgment, 5 August 2015.

such an amendment would "require deep inroads into property law, as many provisions would have to be rewritten" and its legal consequences would need to be considered "very carefully", because "property law not only regulates ownership of property, but also real estate, limited rights in rem such as easements and burdens, as well as mortgages and so on". The Government decided instead to establish an autonomous regime for property-like rights in tokens that were supported by "trustworthy technology".[91]

- In Germany, where the courts have confirmed that data is not a "thing" for the purposes of the property law regime under the Civil Code, the 2021 Electronic Securities Act expressly provides that "crypto securities" within the meaning of that legislation are "things" for the purposes of that regime.

- In China, it has been suggested in legal doctrine that an "online virtual asset" within the meaning of article 127 of the General Provisions of the Civil Law (now article 127 of the Civil Code) includes electronic records maintained on an information network, such as online game accounts and equipment, email and cryptocurrency.[92] Moreover, recent case law suggests that cryptocurrency can be protected by the law of property. In a 2019 decision concerning a claim for property damage following the shutdown of a cryptocurrency exchange, the Hangzhou Internet Court in Zhejiang province referred to the substance of article 127 of the General Provisions of the Civil Law and found that Bitcoin was the object of property rights under the law of China.[93] It reasoned that, in order to be an object of property rights, a unit of cryptocurrency must have value, scarcity and controllability, and that not only Bitcoin but also other tokens and cryptocurrencies possessed each of these features.

- In the Russian Federation, amendments to the Civil Code in 2019 introduced the concept of "digital rights" as an object of civil law rights.[94] The concept of "digital rights" is in turn defined in article 141.1 of the Civil Code as claims and other rights, the content and conditions of implementation of which are determined in accordance with the rules of the information system that meets the requirements of law. The concept of "digital right" would seem to capture digital tokens and thus establish certain digital assets as an object of property rights.

[91] *Report and Application of the Government to the Parliament of the Principality of Liechtenstein concerning the Creation of a Law on Tokens and TT Service Providers (Tokens and TT Service Provider Act; TVTG) and the Amendment of Other Laws,* No. 54/2019, 7 May 2019.

[92] Zhang Xinbao, *Commentary on the General Provisions of the Civil Law* (2017, Renmin University Press).

[93] *Wu Qingyao v. Shanghai Yaozhi Network Technology Co., Ltd. and Zhejiang Taobao Network Co., Ltd.*, Judgment, 18 July 2019.

[94] Russian Federation, Federal Law No. 34-FZ of 18 March 2019 on amendments to parts 1, 2 and article 1124 of part 3 of the Civil Code of the Russian Federation.

93. The question as to whether digital assets in the form of cryptocurrency are "property" has been considered, and in some cases confirmed, by the courts in several common law jurisdictions:

- In Canada, in a 2018 decision, the Supreme Court of British Columbia ordered by summary judgment that Ether tokens be traced in claims for conversion (i.e. a claim for the wrongful interference with property) and wrongful detention, each of which depends on the existence of "goods". While the court granted the remedy, it noted that the proper characterization of cryptocurrencies was "a central issue" in the case and that "the evidentiary record [was] inadequate to permit a determination of that issue" and, in any event, that it raised "a complex and as of yet undecided question that is not suitable for determination by way of a summary judgment application".[95]

- In Singapore, the first instance court in the *Quoine* case found that property rights could subsist in Bitcoin by applying the statement of Lord Wilberforce in the case of *National Provincial Bank v. Ainsworth* (*"Ainsworth"*) before the House of Lords of the United Kingdom that a right claimed to be "property" must be "definable, identifiable by third parties, capable in its nature of assumption by third parties, and have some degree of permanence or stability".[96] On appeal, the Court of Appeal refused to express a final opinion on the question, although it did state that "[t]here may be much to commend the view that cryptocurrencies should be capable of assimilation into the general concepts of property", while acknowledging that there are "difficult questions as to the type of property that is involved".[97] In a subsequent case, the High Court of Singapore held that Bitcoin and Ether were capable of giving rise to property rights that could be protected by an interim injunction prohibiting third-party dealings in those cryptocurrencies.[98]

- In the United Kingdom, the High Court of England and Wales ruled in a 2019 judgment in the case of *AA v. Persons Unknown* that Bitcoin was property for the purposes of granting a proprietary injunction to restrain dealings in the cryptocurrency by a subsequent holder.[99]

- In New Zealand, the High Court held in a 2020 judgment in the case of *Ruscoe v. Cryptopia Limited (in liquidation)* that various cryptocurrencies

[95] *Copytrack Pte. Ltd. v. Wall*, Docket No. S183051, Oral Reasons for Judgment, 12 September 2018, 2018 BCSC 1709.

[96] Singapore International Commercial Court, *B2C2 Ltd. v. Quoine Pte. Ltd.*, Suit No. 7 of 2017, Judgment, 14 March 2019, [2019] SGHC(I) 03, para. 142, citing House of Lords, *National Provincial Bank v. Ainsworth*, Judgment, 13 May 1965, *Official Law Reports: Appeals Cases*, vol. 1965, No. 1, p. 1248.

[97] *Quoine Pte. Ltd. v. B2B2 Ltd.*, Civil Appeal No. 81 of 2019, Judgment, 24 February 2020, *Singapore Law Reports*, vol. 2020, No. 2, p. 20, [2020] SGCA(I) 02, para. 144.

[98] *CLM v. CLN*, Suit No. 470 of 2021, Judgment, 4 March 2022, [2022] SGHC 46.

[99] *AA v. Persons Unknown*, Case No. CL-2019-000746, Judgment, 13 December 2019, *Weekly Law Reports*, vol. 2020, No. 4, [2019] EWHC 3556 (Comm).

held by a cryptocurrency exchange were property for the purposes of company law, and suggested that they could also be property for the purposes of the common law.[100] In coming to this conclusion, the court found that that the cryptocurrencies in that case "clearly met" the requirements of property referred to in the statement by Lord Wilberforce in the *Ainsworth* case.[101]

94. In several of these cases, the courts referred to a legal statement issued by the UK Jurisdiction Taskforce on digital assets and smart contracts.[102] The statement concludes that digital assets possess all the characteristics of property under English common law (as established by Lord Wilberforce in the *Ainsworth* case and in subsequent cases), namely definability, identifiability, capability of assumption by third parties, certainty, control, exclusivity, assignability, permanence and stability. Moreover, it argues that digital assets should not be disqualified as property on the basis alone that they are represented by data and that the English courts have traditionally been reluctant to treat information in itself as property. In this respect, the statement observes that, in the case of digital assets, "it is not what the data tells you but what it allows you to do".[103] In *AA v. Persons Unknown*, the High Court of England and Wales noted that the legal statement represented "an accurate statement as to the position under English law".[104]

- In the United States, it has been suggested in legal doctrine that the 2003 judgment of the Court of Appeals for the Ninth Circuit in the case of *Kremen v. Cohen* provides support for the proposition that cryptocurrency constitutes an object of property rights. In that case, the court accepted that the claim for conversion under the law of California applied to intangible objects – in that case, a domain name – and applied a three-part test to determine whether a property right existed in such an object: (i) there must be an "interest capable of precise definition"; (ii) it must be "capable of exclusive possession or control"; and (iii) "the putative owner must have established a legitimate claim to exclusivity".[105]

95. It is worth highlighting that the UNIDROIT Principles on Digital Assets and Private Law, which are designed to guide law reform in all legal systems, explicitly state that digital assets are capable of being the object of property rights. Commentary on the principles advise jurisdictions to legislate accordingly.

[100] *Ruscoe v. Cryptopia Limited (in liquidation)*, Case No. CIV2019-409-000544, Judgment, 8 April 2020, *New Zealand Law Reports*, vol. 2020, No. 2, p. 809, [2020] NZHC 728.

[101] Ibid., para. 102.

[102] "Legal Statement on Cryptoassets and Smart Contracts", November 2019.

[103] Ibid., para. 60.

[104] *AA v. Persons Unknown*, para. 61.

[105] *Kremen v. Cohen.*, Case No. 0115899, Judgment, 25 July 2003, *Federal Reporter, Third Series*, vol. 493, p. 1030.

(b) Digital assets in the form of asset-backed digital tokens

96. For digital assets in the form of asset-backed digital tokens, the focus of enquiry may turn from the digital asset itself to the linked asset. While the existence of property rights in the linked asset itself might not be problematic (after all, the asset itself may not be an object that is new to property law), questions may arise as to (i) whether the holding of the token can confer rights in the linked asset and (ii) whether transferring the token to another person can lawfully transfer to that person the rights in the linked asset. More so than property law, these issues engage issues of the law of negotiable instruments and negotiable documents, which is addressed separately below.

97. In some cases, the linked asset may be in electronic form (e.g., a digital file linked to an NFT). In such a case, a question may arise as to whether the linked asset is an object of property rights (recalling the discussion in part two of this taxonomy on the treatment of data under existing property law regimes).

- In China, this question was addressed by the Hangzhou Internet Court in a copyright infringement case involving a digital image linked to a DLT-based NFT. In a 2022 judgment, the court found that, owing to the rules of the system that linked the token to the digital image and provided for the transfer of the token, the digital image itself constituted an "online virtual asset".[106]

98. In other cases involving NFTs, a question may instead arise as to whether property rights subsist in the token (i.e., the digital asset), which essentially raises similar issues (explored above) as to whether digital assets in the form of cryptocurrency are "property".

- In Singapore, this question was addressed by the High Court in a case concerning an NFT linked to a digital image. In a 2022 judgment, the court clarified that it was dealing with a token that contained merely "a link to the server where the actual image itself can be found", rather than the digital image, and noted that it raised "similar issues" to the earlier *Quoine* case concerning Bitcoin and Ether. Consistent with its judgment in the earlier case, the court found that the NFT was capable of giving rise to property rights that could be protected by an interim injunction prohibiting third party dealings in the NFT.[107]

[106] Hangzhou Internet Court, *Shenzhen Qicedie Cultural Creativity Co. Ltd. v. Hangzhou Yuanyuzhou Technology Co. Ltd.*, Zhe 0192 Min Chu No. 1008, Judgment, 20 April 2022.

[107] *Janesh s/o Rajkumar v. Unknown Person*, Summons No. 1800 of 2022, Judgment, 21 October 2022, [2022] SGHC 264.

3. Securities law

99. Some digital assets – notably security and investment tokens – purport to confer rights on the holder that resemble the kinds of rights comprised in shares and other investment securities. As such, these digital assets could constitute investment instruments and engage laws relating to the issuance of and trading in investment securities, as well as laws on the holding of securities.

4. Secured transactions law

100. For digital assets in the form of cryptocurrency, the holder may wish to encumber the digital asset (i.e. grant a security interest in the digital asset to secure payment or the performance of some other obligation). This raises a question as to whether the digital asset can be encumbered under secured transactions law. In this regard, the material scope of secured transactions law may be linked to the property law regime, such that only objects of property rights can be encumbered.[108] Further questions arise as to whether the provisions of secured transactions law – including provisions on the perfection and enforcement of the security interest – are adapted to the use of such digital assets as collateral.

101. For digital assets in the form of asset-backed digital tokens, the token may purport to represent a security interest in the linked asset. This raises the question as to whether and how the creation and transfer of the token in the system constitutes the creation and transfer of the security interest, and whether and how the security interest is perfected, and thus made effective against a transferee of the linked asset.

5. Law of negotiable instruments and negotiable documents

102. Some digital assets in the form of asset-backed digital tokens – particularly those that purport to represent rights to delivery of goods or rights to payment – may resemble negotiable instruments such as bills of exchange or promissory notes or negotiable documents such as bills of lading or other documents of title. A question thus arises as to whether existing laws on the use of negotiable instruments and negotiable documents apply to such digital assets, which will depend in large part on whether those laws apply in an electronic environment (an issue that is addressed by the adoption of the MLETR).

[108] For instance, in Australia, the secured transactions law applies to "personal property": *Personal Property Securities Act 2009*, sect. 10.

103. If existing laws do not apply to such digital assets, it is unlikely that the rights that the token purports to represent will have effect beyond the contractual relationship between the person who issued the token and the person to whom the token was initially issued.

6. Other laws

104. Similar questions arise as to whether digital assets in the form of cryptocurrency form part of an insolvency estate. Additional complexity may arise if the digital asset is held by an intermediary such as a cryptocurrency exchange or "wallet" service provider.

105. Other legal regimes with links to property law may be engaged by the use of digital assets, including the law of succession and the law of trusts, as well as sale of goods law. Moreover, digital assets raise questions about the application of remedies such as civil asset tracing.

7. Private international law

106. DLT-based digital assets raise private international law issues, particularly given the geographic distribution of nodes that maintain the ledger in which the data constituting or representing the digital asset is recorded. Given the differences in legal treatment of digital assets across jurisdictions, choice of law rules may play a significant role in determining the rights and obligations of the parties transacting in those assets.

E. Relevant UNCITRAL texts

1. Electronic commerce texts

107. Digital assets are essentially a collection of data messages within the meaning of the MLEC and other UNCITRAL texts on electronic commerce. The rules in part one of the MLEC that give legal recognition and admissibility to data messages are thus relevant to support the use of digital assets. The rules in part two of the MLEC are also relevant to digital assets in the form of electronic transport documents. The rules in the MLETR are also relevant to giving legal effect to tokens purporting to constitute negotiable instruments or negotiable documents.

2. United Nations Convention on Contracts for the International Sale of Goods

108. The CISG applies to the sale of "goods".[109] It does not apply to the sale of "investment securities, negotiable instruments or money".[110] As a collection of data messages, the applicability of the CISG to digital assets as "goods" raises issues similar to those raised by the application of the CISG to data, which is addressed in part two of this taxonomy. With regard to digital assets in the form of cryptocurrency, a further question arises as to whether cryptocurrency is "money" and thus excluded from scope. With regard to digital assets in the form of security or investment tokens or electronic transferable records, a similar question arises as to whether the exclusion of "investment securities" and "negotiable instruments" applies in the electronic environment. If, ultimately, digital assets are "goods" within the meaning of the CISG, a separate question is whether the issuance or exchange of digital assets involves a "contract of sale".

109. It is one thing for a digital asset to be the subject of a sale; it is another for a digital asset to be the means of exchange for goods. A question thus arises whether the transfer of digital assets in the form of cryptocurrency constitutes "payment of the price" for the purposes of the CISG, and whether the transaction can properly be characterized as a "sale". In this regard, if cryptocurrencies are viewed as commodities, the transaction may be regarded as a barter, and the preponderant view in legal doctrine is that a barter contract, under which goods are exchanged for goods or services, share some – but not all – of the elements of a contract of sale.

110. It goes without saying that the CISG was not negotiated with digital assets in mind. If, as a matter of treaty interpretation, the CISG were to apply to digital assets – either as goods or as a means of exchange – yet a further question arises as to whether the rules that it contains are appropriate and adapted to transactions involving digital assets.

3. Secured transactions texts

111. The UNCITRAL Model Law on Secured Transactions (MLST) applies to security interests created in "movable assets", which are defined to include both tangible assets and intangible assets. A "tangible asset" includes money, negotiable instruments, negotiable documents and certificated non-intermediated securities (article 2(ll)), while an "intangible asset" means any movable asset that is not a tangible asset. The

[109] CISG, art. 1(1).
[110] CISG, art. 2(d).

MLST provides for the creation, third-party effectiveness and priority of security rights, and contains specific rules for particular types of assets.

112. The MLST was not developed with digital assets in mind. A question thus arises as to whether the MLST applies to secured transactions involving digital assets and, if so, which specific rules apply. One view is that the rules applicable to intangible assets (instead of the asset-specific provisions) could extend to digital assets, including cryptocurrency and asset-backed digital tokens (e.g., digital tokens constituting investment securities or transferable records).[111] Otherwise, rules specific to digital assets might need to be developed, taking into account the interest of the various actors involved in secured transactions using digital assets as collateral.[112]

4. Insolvency texts

113. The suite of UNCITRAL model laws on insolvency[113] comprises a cooperative and coordinating framework for States to effectively address insolvencies where the debtor has assets in multiple States or where creditors are not from the State in which the proceeding is taking place. The overall goal of the model laws is to provide an expedited, predictable and transparent mechanism to preserve economic value in cases of cross-border insolvency.

114. The model laws focus on the insolvency estate, which is defined to include all assets of the debtor that are subject to the insolvency proceedings. However, the model laws do not delimit the types of assets that fall within the insolvency estate. Further guidance in that regard is set out in the UNCITRAL *Legislative Guide on Insolvency Law*, which provides a comprehensive statement of the key objectives and principles that should be reflected in a modern insolvency law. Specifically, the guide recommends that the insolvency law should specify the assets to be included within the insolvency estate, which are in turn intended to comprise "property, rights and interests of the debtor, including rights and interests in property, whether or not in the possession of the debtor, tangible or intangible, movable or immovable, including the debtor's interests in encumbered assets or in third party-owned assets" (see recommendation 35). This broad definition, coupled with the objectives of an efficient insolvency law, indicate that the debtor's assets may be expected to include digital

[111] This view was expressed by Koji Takahashi in his address to the 2017 UNCITRAL Congress: "Implications of the Blockchain Technology for the UNCITRAL Works", in *Modernizing International Trade Law to Support Innovation and Sustainable Development* (Vienna, United Nations, 2017), pp. 84–87.

[112] For further discussion on the application of the MLST to DLT-based digital assets, see World Bank, *Distributed Ledger Technology & Secured Transactions: Legal, Regulatory and Technological Perspectives – Guidance Notes Services* (Washington, 2020).

[113] UNCITRAL Model Law on Cross-Border Insolvency, UNCITRAL Model Law on Recognition and Enforcement of Insolvency-Related Judgments and UNCITRAL Model Law on Enterprise Group Insolvency.

assets, as permitted by applicable law, whether such assets are held directly or by intermediaries. Further work by UNCITRAL on civil asset tracing and recovery tools used in insolvency proceedings indicates that factors such as the type of digital asset, and the way in which it was created and is held, may further inform the determination of whether the digital asset should be included in the insolvency estate.

115. Once the assets to be included in the insolvency estate have been identified, the insolvency representative must be empowered to establish control over those assets, for example, for the purposes of reorganization or liquidation. This requirement could give rise to additional issues, such as gaining access to the digital asset, and dealing with restrictions on the transferability of digital assets or limits on their use to raise capital.

116. In addition, if the insolvent debtor's assets include digital assets, the location of such assets is not likely to be restricted to the State in which the insolvency proceedings are taking place, thus raising issues of cross-border insolvency.

Part four.

Online platforms

A. Relevance to international trade

117. Online platforms (also known as "digital platforms" or "electronic platforms") are increasingly being used for trade. With the help of enhanced data processing and advanced algorithms, online platforms enable and facilitate the supply of goods and services, connect global supply chain participants, and create virtual spaces or "ecosystems" for sharing and collaboration. Employing a range of systems and technologies, while also pursuing a range of business models, online platforms not only create new trading opportunities, but also new ways of trading. The potential of online platforms for trade is particularly acute for MSMEs.

118. Together with data, online platforms are driving the expansion of the digital economy.[114] Electronic commerce (e-commerce) platforms play an important role in that expansion, accounting for a significant proportion of both business-to-consumer (B2C) and business-to-business (B2B) digital trade, and contributing to a blurring of the lines between the two. Meanwhile, supply chain platforms represent value in terms of the increased efficiencies for users.

B. What is an online platform?

119. The OECD defines the term "online platform" as "a digital service that facilitates interactions between two or more distinct but interdependent sets of users (whether firms or individuals) who interact through the service via the Internet".[115] Using the language of existing UNCITRAL texts on electronic commerce, a working definition based on the OECD definition may be formulated in terms of a service that (i) is provided via the Internet or some other communications network by electronic means (i.e. an online service) and (ii) facilitates interactions between persons who interact using the service. A description of online platforms is given in similar terms

[114] UNCTAD, *Digital Economy Report 2019: Value Creation and Capture – Implications for Developing Countries* (Geneva, 2019), p. xv.

[115] OECD, *An Introduction to Online Platforms and Their Role in the Digital Transformation* (Paris, 2019), p. 21.

by UNCTAD in its *Digital Economy Report 2019*[116] and in a joint publication of ITU and the World Bank on digital regulation.[117]

120. Using this working definition, services provided by online platforms may be distinguished from other online services, which are commonly referred to as "platforms", but which do not involve interactions between multiple users of the service. Online platforms may also be distinguished from software environments and networked environments (e.g., the infrastructure layer of a DLT system), which may also be referred to as "platforms", but which do not involve the provision of an online service (although the application layer of a DLT system may support an online platform). For more on DLT systems, see part five of this taxonomy.

121. The working definition covers a wide variety of online platforms in terms of the number of users, and the type and economic value of transactions that they facilitate. Platforms with a particular significance for trade include:

- *E-commerce platforms* – online platforms that facilitate transactions involving the supply of goods and services. While commonly associated with "online marketplaces" used for the supply of goods to consumers, e-commerce platforms facilitate B2B transactions, including the supply of financial services (e.g., crowdfunding and trade finance platforms) and digital products, and support the management of contracts under which goods and services are supplied.
- *Dispute resolution platforms* – online platforms that facilitate the resolution of disputes by providing a system for the exchange of electronic records and communications between parties (including case management and remote hearings).
- *Supply chain platforms* – online platforms that facilitate interactions between supply chain participants, including the transfer of dematerialized trade documents (e.g., electronic transport records, certificates of origin and bills of exchange). Legal issues related to digital assets are explored in part three of this taxonomy. Supply chain platforms also provide a space for users to share (or "pool") supply chain data. Legal issues specific to data sharing and other data transactions are explored in part two of this taxonomy.[118]

[116] UNCTAD, footnote 114 above, p. xv (referring to "digital platforms" as providing "the mechanisms for bringing together a set of parties to interact online").

[117] *Digital Regulation Handbook* (Geneva, 2020), p. 31 (referring to "digital platforms" acting "as a marketplace, bringing together and reducing transaction costs between distinct groups of customers").

[118] The types of platforms are not mutually exclusive; for instance, a supply chain platform may facilitate the provision of trade finance and logistics services.

122. The working definition is formulated in technology- and system-neutral terms, and thus covers platforms employing a range of systems and technologies, including the use of interactive applications (e.g., to support communication between platform users), distributed ledger technology and associated applications (e.g., to record transaction data), and the deployment of AI and other automated systems (e.g., to optimize the user experience).

123. It also covers platforms that offer additional services to users, which may be provided on or off the platform.

- For e-commerce platforms, additional services may include advertising services, ranking and reputation systems, payment services, identity management (IdM) and other trust services, and logistics services. They may also include a system for handling complaints, as well as a system for resolving disputes between users (in which case the platform would also be a dispute resolution platform).
- For dispute resolution platforms, additional services may include the deployment of AI and other automated systems with the aim of expediting the dispute resolution process. These systems may be deployed to generate possible terms of settlement (e.g., by analysing data of past disputes) or to enforce the outcome of the process. They may also be deployed to inform or determine the outcome of the dispute resolution process itself (e.g., AI decision-making).
- For supply chain and dispute resolution platforms, additional services may include registry services.

124. The provision of additional services may lead to the platform operators playing a more active and influential role in the interactions between users. In a similar vein, the working definition also covers online platforms where the platform operator itself uses the platform to interact with users. For instance, the operator of an e-commerce platform may offer goods and services to users in competition with other users.

125. Given the variety of online platforms, some jurisdictions have opted not to enshrine a definition in law when seeking to regulate online platforms.[119] However, several legislative initiatives dealing with e-commerce platforms have attempted to do so.

- An early jurisdiction to legislate a definition was France with the enactment of the Law No. 2015-990 of 6 August 2015. This law inserted article L111-5-1 into the Consumer Code, which imposed certain information requirements on persons operating an "intermediation service" consisting

[119] See, e.g., legislation regulating digital platforms under part IVBA of the *Competition and Consumer Act 2010* of Australia.

of putting several parties in contact by electronic means with a view to the supply, exchange or sharing of goods and services. Following the enactment of Law No. 2016-1321 of 7 October 2016 (the "Law for a Digital Republic"), the definition is now found in article L111-7(I)(2) of the Consumer Code.

- In China, the Electronic Commerce Law (2019) regulates "e-commerce platform operators", which are defined to mean a person providing the services of "network operational space, transactional matchmaking, and information dissemination for the parties to carry out bilateral or multi-lateral transactions independently".

- In the European Union, the Platform-to-Business (or P2B) Regulation[120] regulates "online intermediation services", which it defines as online services, provided on a contractual basis, which "allow business users to offer goods or services to consumers, with a view to facilitating the initiating of direct transactions between those business users and consumers, irrespective of where those transactions are ultimately concluded".

- In India, the *Consumer Protection (E-Commerce) Rules, 2020*, made under the *Consumer Protection Act, 2019*, regulate "e-commerce entities" which own, operate or manage "platforms" for e-commerce. The term "platform" is defined to mean "an online interface in the form of any software including a website or a part thereof and applications including mobile application". The rules regulate the use of platforms by e-commerce entities not only (i) to "facilitate transactions between buyers and sellers" (referred to as "marketplace e-commerce entities"), but also (ii) to sell goods and services directly to consumers (referred to as "inventory e-commerce entities").

- In Japan, the Act on Improving Transparency and Fairness of Digital Platforms (Act No. 38 of 2020, also known as the "TFDPA") defines "digital platforms" as online spaces for parties to connect.

- In the Russian Federation, amendments to the Law on Consumer Rights Protection by Federal Law No. 250-FZ of 29 July 2018 introduced the concept of an online "aggregator", which is defined as a computer program, website or web page that allows a consumer: (i) to obtain information about offers of goods and services from suppliers; (ii) to enter contracts with suppliers for the supply of goods and services; and (iii) to make advance payments for the goods or services to the owner of the aggregator.

[120] Regulation 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (P2B Regulation).

126. In addition to these legislative initiatives, the European Law Institute has developed Model Rules on Online Platforms that aim to "consolidate existing European and national legislation" and to "provide some innovative solutions for issues that could be addressed in forthcoming regulatory initiatives".[121]

127. While some of the definitions formulated for e-commerce platforms in the various jurisdictions are broader than the working definition, they all contemplate the use of platforms as an online service that facilitates interactions (in the form of electronic transactions) between third parties directly via the platform (even if part of the transaction is carried out off the platform). This understanding may also be applied to other online platforms, such as supply chain platforms and dispute resolution platforms.

C. Actors

128. At a basic level, an online platform involves two types of actors:

- *Platform operator* – the person who provides the online service constituting the platform, including by deploying the software supporting the online space created by the platform.
- *Platform user* – the person who uses the platform to interact with others.

129. Platforms establish a "community" of users that interact in a variety of capacities depending on the platform.

- For e-commerce platforms, the community of users will generally comprise buyers and suppliers of goods or services, who may engage in those activities in the course of business (business users) or for personal, family or household purposes (i.e. as consumers).
- For dispute resolution platforms, the community of users will generally comprise the parties to the dispute, an arbitrator or mediator, and other persons involved in the dispute resolution process (e.g., expert witnesses). As noted above (section B), the platform operator may also play an active role in the dispute resolution process through the deployment of additional AI-enabled services.
- For supply chain platforms, the community of users will generally comprise participants in the supply chain, including producers, distributors, transporters and conformity assessment bodies.

[121] Available at www.europeanlawinstitute.eu/projects-publications/completed-projects-old/online-platforms/.

130. The platform operator will generally be a legal person providing the online service in the course of business. An online platform may also be established or controlled by a public authority. As noted above (section B), the platform operator may also use the platform to interact as a platform user.

131. If the online platform offers additional services, the provider of those services – if not the platform operator itself – will be an additional actor. Third party providers of those services are not generally users of the platform. Other actors include third parties with intellectual property in material that is made available on the platform, as well as manufacturers and producers of goods that are sold on the platform. For some online platforms, regulatory authorities may be relevant actors so far as they set rules for the platform and enforce compliance with those rules and other regulatory requirements.

D. Legal regimes

1. Contract law

132. The various actors in an online platform are connected by a series of contractual relationships. A contract will generally be concluded between the platform operator and each platform user, which incorporates the terms of use for the platform (i.e. the platform rules). The terms of the contract may vary on account of the capacity in which the user interacts through the platform, including any additional services that it uses. One or more contracts may also be concluded between users in the course of their interaction via the platform. Depending on the platform, those contracts may include contracts for the sale of goods, contracts for the supply of services, or cooperation agreements.

133. It follows that contract law, including general principles such as good faith and fair dealing, as well as the terms of the contract agreed by the parties under the principle of freedom of contract, will be a primary source of the rights and obligations among the various actors involved in an online platform.

- The application of the principle of good faith to relations between platform operator and user was considered in a case in Japan concerning fraudulent transactions carried out on an online auction platform. In that case, the Nagoya District Court decided that the principle of good faith required that, in discharging its contract with users, the platform operator needed to build a system that was "without defect" for the sake of those users.[122] In coming to that decision, the court considered a

[122] Nagoya District Court, Judgment, 28 March 2008, Case No. 2005 (Wa) 1243, *Hanrei Jiho*, vol. 2029, p. 89.

> variety of factors, including the social circumstances surrounding online auctions at the time when the service was provided, technical standards of the system, the cost of structuring and maintaining the platform, and the effect of introducing the platform and the convenience for users.[123]

134. A preliminary issue relates to isolating the contracts involved in the operation of an online platform. An example of that issue is provided by the *Quoine* case before the courts of Singapore, which involved trading contracts between users of QUOINExchange, a cryptocurrency exchange platform. The user in that case (B2C2) argued that the trading contracts were part of a "spider's web" of contracts, with the operator (Quoine) as a central counterparty to both sides of the trade. Conversely, the operator argued that the trading contracts were formed directly between users. The Singapore International Commercial Court agreed with the latter argument.[124] In doing so, the court described what is sometimes referred to as the "triangular" contractual structure of online platforms.

135. Further issues relate to contracts being concluded online via the platform and therefore (i) by exchange of electronic communications (i.e. communications by means of data messages), (ii) between parties at a distance and (iii) depending on the platform, without human intervention. While none of those issues is specific to online platforms, the prevalence of online platforms for electronic contracting in general, and automated contracting in particular, may give these issues special prominence.

- Electronic transactions laws have been enacted in most jurisdictions to recognize that a contract may be concluded by exchange of electronic communications, and that a legal requirement for the contract to be in writing may be met by electronic communications. In many of those jurisdictions, such laws are based on the MLEC. A related issue is the extent to which the use of interactive applications (e.g., the click of a button on a website in a "click-wrap" scenario) – or indeed continued use of the platform (e.g., in a "browse-wrap" scenario) – can constitute acceptance by a party of the terms offered by the counterparty. That may in turn depend on the design and operation of the platform. In some jurisdictions, case law confirms the valid conclusion of a contract using these applications. Another related issue is the availability of the terms of the contract.
- The design or operation of the platform may make it difficult for a user to identify the counterparty to a contract concluded via the platform. And once identified, the counterparty may be difficult to locate, or may be located in another jurisdiction. Moreover, the user may require the identity of the counterparty

[123] Cited in the interim discussion paper of 12 December 2018 of the study group on improvement of trading environment surrounding digital platforms.

[124] Singapore International Commercial Court, *B2C2 Ltd. v. Quoine Pte. Ltd.*, Suit No. 7 of 2017, Judgment, 14 March 2019, [2019] SGHC(I) 03, paras. 126, 131. On appeal, the Court of Appeal of Singapore agreed with this analysis: Singapore, *Quoine Pte. Ltd. v. B2B2 Ltd.*, Civil Appeal No. 81 of 2019, Judgment, 24 February 2020, *Singapore Law Reports*, vol. 2020, No. 2, p. 20, [2020] SGCA(I) 02, para. 50.

to be verified (whether to satisfy a legal obligation or otherwise) and the platform operator may provide IdM services to users. A question therefore arises as to whether the use of IdM services will be recognized by applicable law (e.g., to satisfy the legal obligation for identification, or for the application of some other law, such as an obligation of due diligence, for which verification of identity or particular identity attributes may be relevant).

- Legislation has been enacted in some jurisdictions to recognize that a contract may be concluded by use of an automated system (or "electronic agent") without human intervention. The use of automated systems in contracting is explored in part one of this taxonomy.

136. The terms of use incorporated into the contract between the platform operator and the platform user will generally be the primary vehicle by which the governance framework for the platform is established. The platform rules will not only govern the relations between the platform operator and platform user, but also the interactions between the user and other platform users. The governance framework may give rise to additional contract law issues, including (i) the ability for the platform operator to modify the terms of use unilaterally and (ii) the extent to which the platform operator can "enforce" the platform rules by invoking penalty clauses contained in the terms of use against a non-compliant user (e.g., preventing the non-compliant user from accessing the platform, or downgrading or limiting visibility of goods and services offered by the user). While, again, none of these issues is specific to online platforms, the special nature of the terms of use and the position of influence that they afford the platform operator in relation to the user and interaction among users may give the issues special prominence, even for business users.

- Applicable law will usually require modifications to be accepted by the counterparty (i.e. the platform user). In the context of online platforms, this requirement may be satisfied by the user clicking a button on a website in a "click-wrap" scenario, or by the user continuing to use the platform after being notified of the modifications.[125] However, applicable law – including rules on unfair contract terms, the doctrine of unconscionability and public policy considerations – may limit the types of modifications that can be made and the circumstances in which they may be accepted, particularly if the platform operator offers the online service on the basis of standard, non-negotiable terms of use.

- Applicable law may also limit the use of penalty clauses.

[125] The issue of unilateral modification was considered in the *Quoine* case in Singapore, in which the Court of Appeal noted that, under applicable law, the platform user had to have "reasonable means of knowing that there had been a modification to the terms and what that modification was before any such change could have legal effect": footnote 124, para. 62.

- In a case in China, the Shanghai No.1 Intermediate Court decided in a 2020 judgment that, having regard to the interests of consumers and the promotion of electronic commerce, it was reasonable for a platform operator to deduct a sum of money from a user supplying counterfeit goods via the platform as compensation to affected consumers.[126]

137. Similar laws may also constrain the ability of the platform operator to include other provisions in the terms of use, such as choice of court clauses (for a discussion on private international law issues, see subsection D.6 below).

138. Given the data-intensity of online platforms, which process data collected from or generated by users, including through their interactions through the platform (e.g., transaction data), the terms of use incorporated into the contract will also address the rights and obligations of the parties in that data. The contractual issues relating to these rights and obligations are addressed in part two of this taxonomy.

2. Tort law

139. Tort law may also affect the legal rights and obligations among the various actors involved in an online platform. In particular, tort law – understood broadly to encompass extra-contractual obligations however classified under applicable law – will generally serve as a basis for claims against the platform operator arising from the conduct of a platform user on the platform. For instance, a person may bring a claim for the provision of inaccurate, incomplete and misleading information (e.g., information about the platform, the platform operator or the platform rules), for interference with intellectual property (e.g., copyrighted material made available to users on the platform without permission of the copyright owner), for infringement of reputation or privacy (e.g., defamatory material or personal data accessible to users on the platform), or for interference with property (e.g., a digital asset supported by the platform erroneously transferred to a third party). The claim may rely on the liability of the platform operator for the conduct of the platform user (e.g., joint liability or vicarious liability), or for the intervening conduct of the platform operator (e.g., "publication" of defamatory material posted by the user).

140. A platform operator may seek to limit its liability by invoking an indemnity clause in the terms of use against the platform user (such clause forming part of the governance framework for the platform), or relying on "safe harbour" legislation under the applicable law.

[126] Shanghai No.1 Intermediate Court, *Jingdezhen Jinlin Business and Trade Co., Ltd. v. Shanghai Xuemeng IT Co., Ltd.*, Hu 01 Min Zhong No. 3224, Judgment, 24 April 2020.

- The law that limits modifications and penalties (discussed in in subsection D.1) may also limit the ability of the platform operator to rely on the indemnity clause.
- "Safe harbour" legislation has been enacted in many jurisdictions to shield online service providers from liability arising from user-generated content that they host, on the condition that the provider has no knowledge or awareness of the offending content, or acts expeditiously to remove the content.
- While some legislation applies to content that infringes copyright,[127] other legislation is of more general application.[128] As online service providers, platform operators will generally be covered by "safe harbour" legislation. In the European Union, the "safe harbour" provisions of the Directive on Electronic Commerce expressly exclude any obligation on the service provider to monitor the content that they host.[129] However, case law has emphasized that those provisions only apply if the platform operator acts as a "neutral" intermediary in the sense that "its conduct is merely technical, automatic and passive, pointing to a lack of knowledge or control of the data which it stores".[130]

3. Laws specific to the interactions facilitated by online platforms

141. Online platforms facilitate a variety of interactions between users to which specific legal regimes may be applicable. For instance, transactions involving the supply of goods might engage sale of goods law, transactions involving consumers might engage consumer protection law, interactions involving services to handle disputes might engage arbitration or other dispute resolution laws, and transactions involving crowdfunding might engage finance and investment laws.

142. Platforms may employ systems that support the creation and transfer of digital assets. For example, supply chain platforms may be used for the creation and transfer of electronic negotiable instruments such as bills of exchange or promissory notes or electronic negotiable documents such as bills of lading or other documents of title.

[127] China, Regulation on Protection of the Right to Network Dissemination of Information, State Council Order No. 468 of 18 May 2006; United States, *United States Code*, Title 17, sect. 512(c).

[128] See, e.g., Brazil, Law No. 12.965 of 23 April 2014, art. 19; European Union, Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on Electronic Commerce), art. 14; India, *Information Technology Act, 2000*, sect. 79; South Africa, *Electronic Communications and Transactions Act, 2002*, ch. 11.

[129] Directive on Electronic Commerce (footnote 128), art. 15.

[130] Court of Justice of the European Union, *Google France SARL v. Louis Vuitton Malletier SA*, Case No. 236/08, Judgment, 23 March 2010, para. 114. Similar reasoning was applied by the Commercial Court of Appeals of Argentina in *Kosten v. Mercado Libre S.R.L.*, Judgment, 22 March 2018, Case No. 34503/2014.

Legal regimes engaged by dealings with digital assets are addressed in part three of this taxonomy.

143. Depending on the platform, it is conceivable that the applicable law will regard the interaction between the platform operator and users as involving a partnership or agency arrangement. A partnership arrangement, which is more likely for a platform establishing a virtual online space for collaboration than an e-commerce platform, would have implications for the rights and obligations between the parties involved. Likewise, an agency arrangement involving one person (the principal) engaging a second person (the agent) to act on behalf of the principal would have implications for the rights and obligations between the parties involved.

144. For dispute resolution platforms, a question arises as to whether the applicable law recognizes the use of electronic records (including expressions of consent, submissions and the outcome of the dispute resolution process) and electronic communications (including remote hearings and communications between the parties), as well as the use of IdM systems to control access to the platform, the use of pseudonyms, or the anonymous use of the platform. A question also arises as to how to translate due process requirements to an online space. In that regard, various international initiatives aim to develop standards for online dispute resolution.

4. Laws specific to online platforms

145. Several jurisdictions have enacted laws that apply specifically to e-commerce platforms.[131] None of the laws seeks to establish a complete, self-contained regime for e-commerce platforms, although they tend to apply as mandatory law, defining rights and obligations of platform operators and platform users from which the parties cannot contractually deviate (e.g., by way of the platform rules).

- In the European Union, the P2B Regulation imposes a range of obligations on platform operators in their relations with "business users" which offer goods or services to consumers. In broad terms, those obligations include (i) ensuring that terms of use that are unilaterally determined by the operator comply with certain information requirements, (ii) ensuring that the terms of use comply with certain minimum content requirements, (iii) giving business users prior notice of any proposed modifications to the terms of use, (iv) providing business users with a statement of reasons for any decision concerning restriction, suspension and termination of the service and (v) providing an effective internal complaints handling system for business users which is accessible and free of charge, and handles complaints within a reasonable time frame.

[131] See also India, *Consumer Protection (E-Commerce) Rules*, 2020.

- In China, the Electronic Commerce Law imposes a range of obligations on the platform operator that are not limited to relations with users supplying goods and services via the platform. In broad terms, those obligations include (i) formulating the terms of use in accordance with principles of fairness, transparency and impartiality and in compliance with certain minimum content requirements, (ii) complying with certain information requirements relating to the terms of use, (iii) consulting users on proposed modifications to the terms of use, and publicizing the modified terms at least seven days before they take effect, (iv) refraining from imposing unreasonable restrictions or conditions on users supplying goods and services with respect to transactions that are carried out via the platform, the price for goods and services supplied, and transactions with other operators, and refraining from collecting unreasonable fees from those users, (v) publicizing measures taken against users supplying goods and services for breach of legal or regulatory requirements (e.g., warnings or the suspension or termination of service), (vi) distinguishing its own business conducted on the platform, (vii) identifying goods and services that are ranked against payment, (viii) ensuring platform security, (ix) refraining from aggregate trading practices in the provision of additional services, and (x) establishing a convenient and effective complaints handling system. In addition, the Electronic Commerce Law permits – but does require – the platform operator to establish a system for the online settlement of disputes between users. It recognizes that disputes may be resolved by negotiation, mediation or arbitration (among other forms of dispute settlement). The Electronic Commerce Law also provides for the platform operator to be jointly liable with a user if (i) the goods or services supplied by the user fail to comply with safety standards or otherwise violate consumer rights, and (ii) the operator knew or ought to have known of that failure or violation and failed to take necessary action.
- In Japan, the TFDPA imposes several obligations on designated platform operators in their relations with users supplying goods and services via the platform.[132] In broad terms, those obligations include (i) disclosing the terms of use for the platform, (ii) giving prior notice to users of any proposed modifications to the terms of use, and (iii) taking measures to promote mutual understanding in the business relationship between the platform operator and user in accordance with guidelines issued by the responsible ministry, including with respect to systems and procedures to ensure the fair operation of the platform and to handle user complaints.
- In the Russian Federation, the Law on Consumer Rights Protection imposes several obligations on e-commerce platform operators in their relations

[132] Three online marketplaces and two app stores have been designated under the TFDPA: www.meti.go.jp/english/press/2021/0401_001.html.

with consumers using the platform, including a requirement to provide those users with information about the identity of the operator and the identity of suppliers using the platform. Moreover, it provides for the platform operator to be liable for loss suffered by a consumer caused by inaccurate or incomplete information provided by the operator (including information about goods and services supplied via the platform). However, it provides that the supplier remains liable for violations of consumer rights.

146. Several jurisdictions have enacted laws that apply specifically to crowdfunding platforms (i.e. platforms that match prospective investors and lenders with persons seeking funding).

- In the European Union, the 2020 Regulation on European Crowdfunding Service Providers[133] acknowledges that crowdfunding platform operators should act as "neutral intermediaries" between platform users. The regulation imposes a range of obligations on platform operators in their relations with users, including an obligation to act honestly, fairly and professionally in accordance with the best interests of users, an obligation to refrain from participating in crowdfunding, an obligation to carry out due diligence requirements in respect of persons seeking investment, and information disclosure obligations to investors.
- In the Russian Federation, Federal Law No. 259-FZ of 2 August 2019 deals with platforms that are used to conclude investment agreements between investors and persons raising investments. The law imposes a range of obligations on platform operators in their relations with users, including minimum content requirements for platform rules, an obligation to refrain from various financial activities, an obligation to retain and disclose contract terms, and information disclosure requirements to investors. Moreover, the law provides rules on liability of platform operators, and rules on the formation of investment agreements between users.

147. While they do differ, these laws pursue a common purpose of addressing the influence of platform operators over the trading activities of platform users, as well as a common objective of rebalancing the relationship through greater transparency and fairness. Overall, they suggest a common view that e-commerce platforms occupy a *sui generis* position in trade that may warrant legislative intervention.

148. The laws are primarily focused on B2C e-commerce platforms, but are not concerned solely with consumer relations. On their terms, the laws in the European

[133] Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European crowdfunding service providers for business, and amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937.

Union, China and Japan apply to the B2B relationship between the platform operator and businesses that use the platform to sell goods and supply services, and the platforms that they regulate are also used by businesses to buy those goods and services (particularly MSMEs). Moreover, the P2B Regulation in the European Union is aimed uniquely at the B2B relationship with business users, even if it recognizes the link between that relationship and consumer welfare. The operation of the various laws tends to support a view that the influence exerted by platform operators over the trading activities of users causes a blurring of the line between B2B relations and B2C relations. Indeed, the principles of transparency and fairness that the various laws pursue are equally relevant to B2B relations.

5. Other laws

149. Even in the absence of specific laws regulating online platforms, the influence that a platform operator exerts over the interactions between platform users may shape the characterization of its relationship with users and its obligations towards them under other laws, including tort law, consumer protection law, competition law and employment law.

- In the United States, the Court of Appeal of California found in a 2020 judgment that a major e-commerce platform operator was liable under the doctrine of strict products liability for a defective product supplied by one user (a seller) to another user (a consumer). Having regard to the "structure" of the operator's relationship with both users, and in particular the warehousing and delivery services that the operator provided to the seller, the court observed that the operator was "a direct link in the chain of distribution, acting as a powerful intermediary between the third-party seller and the consumer", that it exerted pressure on upstream distributors to enhance safety, and that it had the ability to adjust the cost of liability between itself and its third-party sellers.[134]
- In a case concerning the competence of European Union member States to regulate taxis, the Court of Justice of the European Union took the view in a 2017 judgment that the operator of the ride-sharing platform was not merely an intermediary but provided a "service in the field of transport". In coming to that view, the court noted that the operator exercised "decisive influence" over the conditions under which drivers using the platform provided transport services to passenger users, such as determining the maximum fare, receiving the full fare from the passenger

[134] *Bolger v.* Amazon.com, *LLC*, Judgment, 13 August 2020, *California Appellate Reports, Fifth Series*, vol. 53, pp. 431, 438439.

> before paying part of it to the driver, and exercising a certain control over the quality of vehicles, the drivers and their conduct.[135]

150. Competition law issues may also be engaged by platforms that establish a virtual online space for collaboration among participants in a particular market.

151. Online platforms rely on data that is collected from or generated by users. The processing of data by platform operators engages privacy and data protection laws, as well as other protective laws with respect to data that are explored in part two of this taxonomy.

6. Private international law

152. To the extent that online platforms involve the provision of online services or the conclusion of contracts online, existing rules of private international law as applied to the online environment will apply to determine the applicable law and the jurisdiction of courts. In the case of contracts in B2B transactions, those rules will generally accept the law and the court chosen by the parties pursuant to the principle of party autonomy, which choice may in turn be made in the terms of use of the platform so as to establish, as much as possible, a uniform legal environment. Where no choice is made, or where that choice is not accepted, the global reach of online platforms means that the rules of private international law, including rules based on the location of the parties or the location of the relevant conduct, may lead to different laws applying to the use of the same platform. By creating an online space for the parties to interact, online platforms raise the question as to whether new rules of private international law should be developed to promote greater uniformity, including rules based on the location of the platform or platform operator.

E. Relevant UNCITRAL texts

1. Electronic commerce texts

153. In technical terms, online platforms are essentially a system for processing electronic communications among the platform operator and the community of users. As noted above (subsection D.1), electronic communications may be exchanged to conclude contracts (e.g., a contract for the supply of goods or services, or a dispute

[135] *Asociación Profesional Élite Taxi v. Uber Systems Spain SL*, Judgement, 20 December 2017, Case No. 434/15, para. 39. The court did not need to consider whether the operator was itself the provider of the transport services to passenger users.

settlement agreement), to create and transfer digital assets, and to provide digital services. UNCITRAL electronic commerce texts thus apply to give legal recognition to a range of activities carried out on online platforms.

154. UNCITRAL texts also give legal recognition to certain types of digital assets that are created and transferred on online platforms. Specifically, article 10 of the MLETR provides that an electronic transferable record satisfying the conditions of the MLETR shall not be denied legal effect, validity or enforceability on the sole ground that it is in electronic form. Based on the principle of functional equivalence, the MLETR applies the existing law of negotiable instruments and negotiable documents to those electronic records.

2. United Nations Convention on Contracts for the International Sale of Goods

155. To the extent that cross-border transactions carried out via online platforms involve the sale of goods, the CISG may be applicable, even though its drafters would not have had online platforms in mind. The application of the CISG to digital products transacted on online platforms is addressed in part two of this taxonomy.

156. With respect to contract formation, the CISG (articles 11 and 12) does not subject the contract of sale to any requirement as to form and provides that no written agreement is necessary. The ECC (article 20(1)) makes it clear that the electronic communications exchanged by parties to contracts falling under the scope of application of the CISG will benefit from the favourable regime provided by the ECC, which assures that contracts concluded, and other communications exchanged, electronically are as valid and enforceable as their traditional paper-based equivalents.

3. Dispute resolution texts

UNCITRAL Technical Notes on Online Dispute Resolution

157. The earlier work of UNCITRAL on online dispute resolution ("ODR") resulted in the adoption in 2016 of the Technical Notes on Online Dispute Resolution (Technical Notes).[136] This non-binding text is designed to foster the development of ODR and is intended for use in disputes arising from cross-border low-value electronic commerce transactions. The Technical Notes are relevant not only for dedicated dispute resolution platforms, but also dispute resolution systems that are integrated into e-commerce platforms.

[136] Available at https://uncitral.un.org/texts/onlinedispute.

158. The Technical Notes recognize the potential for ODR to offer a simple, fast and efficient process utilizing various forms of dispute resolution (including negotiation, conciliation, mediation, facilitated settlement, arbitration, among others). At the same time, they emphasize that ODR should comply with the same confidentiality and due process standards that apply to offline dispute settlement.

159. The Technical Notes also recognize that ODR involves the following structural elements:

- A "technology-based intermediary" – an "ODR platform" – which is defined as a "system for generating, sending, receiving, storing, exchanging or otherwise processing communications in a manner that ensures data security"; and
- An "ODR administrator", which may be separate from, or part of, the ODR platform, and therefore act as the platform operator or a third party providing additional services on the platform.

160. The Technical Notes describe desirable practices and procedures for resolving disputes using ODR platforms. One such practice is that all communications in ODR proceedings take place via the ODR platform. The Technical Notes also describe desirable practices of the ODR administrator to promote transparency about the platform, and to promote the independence and expertise of third party "neutrals". The term "neutral" is defined as an "individual" who assists the parties in settling or resolving the dispute. They also describe desirable practices for the appointment of neutrals and the conferral of powers.

Other dispute resolution texts

161. While many of the UNCITRAL dispute resolution texts were not drafted with dispute resolution platforms in mind, they are generally flexible enough to accommodate mediation and arbitration conducted in an online space.

- Provisions explicitly recognizing the use of electronic means to satisfy requirement for "writing" and "signature" have found their way into more recent UNCITRAL texts (e.g., arts. 2(2) and 4(2) of the Singapore Mediation Convention).
- When revising the UNCITRAL Model Law on International Commercial Arbitration (MAL) in 2006, two options were provided in article 7 with the first option taking a similar approach to the Singapore Mediation Convention (see article 7(4)) and the second option taking a more flexible approach with no form requirements for arbitration agreements. This also led to the 2006 recommendation regarding the interpretation of article II, paragraph 2,

and article VII, paragraph 1, of the New York Convention,[137] which casts the form requirements in the Convention for an arbitral agreement against the backdrop of the widening use of electronic commerce, including arbitral agreements in electronic form. In parallel, article 20(1) of the ECC makes it clear that electronic communications exchanged in connection with the formation of a contract (including a contract containing an arbitration agreement) benefit from the favourable regime provided by the ECC, which assures that contracts concluded, and other communications exchanged, electronically are as valid and enforceable as their traditional paper-based equivalents. Conversely, for arbitral awards, article 31 of the MAL requires the award to be in writing and to be signed by the arbitrator or arbitrators and does not recognize the use of electronic means to satisfy that requirement.

- More recently, the UNCITRAL Expedited Arbitration Rules expressly authorize the arbitral tribunal to utilize "any technological means as it considers appropriate to conduct the proceedings, including to communicate with the parties and to hold consultations and hearings remotely". The explanatory note clarifies that the inclusion of this provision does not imply that the use of technological means is available to the arbitral tribunal only in expedited arbitration.

[137] Available at https://uncitral.un.org/en/texts/arbitration/explanatorytexts/recommendations/foreign_arbitral_awards.

Part five.

Distributed ledger systems (including blockchain)

A. Relevance to international trade

162. 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 UNCTAD has observed, prominent use cases for DLT-enabled applications are in the areas of online payments, finance, international trade and global value chains.[138] 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".[139]

B. What are distributed ledger systems?

1. Domestic and international definitions

163. 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".[140] Transactions were to be recorded in blocks forming a chain; no reference was made to a "ledger".

164. More recently, ITU has published a technical specification[141] 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

[138] UNCTAD, *Harnessing Blockchain for Sustainable Development: Prospects and Challenges* (Geneva, 2021), p. 5.
[139] World Economic Forum, "Redesigning Trust: Blockchain Deployment Toolkit", April 2021, p. 14.
[140] Satoshi Nakamoto, "Bitcoin: A PeertoPeer Electronic Cash System", 31 October 2008, p. 1.
[141] ITU, *Distributed Ledger Technology Terms and Definitions*, Technical Specification FG DLT D1.1, 1 August 2019.

(the "nodes"). Those technologies and methods include cryptographic techniques (such as 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 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 mechanism".[142] A "DLT system" is in turn defined as a system that implements a distributed ledger.[143]

165. 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.

166. Legislation has been introduced in several jurisdictions with the aim of promoting, recognizing or regulating the use of DLT systems, as well as attracting investment in high-tech industries. In some jurisdictions, legislation defines DLT systems by reference to the technologies and methods deployed to implement and maintain a distributed ledger.

- 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".[144]
- In Italy, Law Decree No 135/2018,[145] 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".
- 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

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

[143] ITU, *Requirements for Distributed Ledger Systems*, Recommendation ITU-T F.751.0, 13 August 2020, para. 3.2.6.

[144] Decree of the President of the Republic of Belarus No. 8 of 21 December 2017 on Development of Digital Economy, annex 1, cl. 8.

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

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".

- In the United Stations, so-called "blockchain enabling" laws have been introduced in several states. In Arizona, the Electronic Transactions Act was amended in 2017 to give legal recognition to certain uses of "blockchain technology", which is defined in the legislation 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".[146] A similar law was enacted in Vermont, which 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".[147] In Illinois, the Blockchain Technology Act 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".[148]

167. By referring to DLT systems variously as "decentralized", "accessible", "permissioned", "permissionless", "public" and "private", these definitions signal the importance of the infrastructure and governance structures of DLT systems to understanding the legal issues that they engage, which are outlined later in this section. In other jurisdictions, more technology-neutral definitions tend to focus on the qualities of data recorded in the distributed ledger resulting from the application of (unspecified) technologies and methods.

- 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 defined in terms of prescribed authentication requirements, namely that the device be operated so as to ensure the integrity of entries.

- In Germany, the 2021 Electronic Securities Act provides for the issuance of securities based on DLT systems ("cryptosecurities"). The legislation 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.

[146] *Arizona Revised Statutes*, title 44, chap. 26.

[147] *Vermont Statutes*, title 12, sect. 1913.

[148] *Illinois Compiled Statutes*, chap. 205, act 730, sect. 5.

- In Switzerland, the Federal Act on the Adaptation of Federal Law to Developments in Distributed Ledger Technology,[149] 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 for the integrity and transparency of data entries therein.
- In the European Union, a proposal to amend the eIDAS Regulation[150] 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".[151]

2. Other ways of defining DLT systems

(a) Defining DLT systems in terms of trust?

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

- 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.
- 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 (see section D below for a discussion about the recognition of trust services in UNCITRAL electronic commerce texts).

169. 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

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

[150] 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.

[151] 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).

avoid non-legal concepts such as immutability and auditability; while those features 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 attributed.

(b) Defining DLT systems in terms of automation?

170. 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 part one of this taxonomy.

(c) Defining DLT systems in terms of platforms?

171. DLT systems are sometimes described as "platforms". Applying the working definition of "online platform" that is elaborated in part four of this taxonomy, 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 the 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 part of the taxonomy avoids referring to DLT systems as "platforms", while acknowledging the use of trade-related DLT-based platforms (i.e. online platforms that integrate DLT systems to support the delivery of services to users).

3. A working definition

172. 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[152] that are deployed to implement and maintain a ledger (or database) that is shared, replicated and synchronized on multiple networked computers (or servers).[153] 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.

173. At their core, DLT systems represent a new way of recording data. Admittedly, 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 technologies are developing. Nevertheless, a focus on the types of data recorded in a distributed ledger is a useful starting point to understand the trade-related applications of DLT systems.

- 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 part four of this taxonomy.
- 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 (subsection E.1).
- 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,[154] which may not have any connection to a commercial activity, or match the concept of transaction under domestic law.[155]

[152] The term "method" is used here in the same sense as it is used in UNCITRAL electronic commerce texts.

[153] Legal doctrine and legislation often conflate the terms "DLT" and "blockchain"; for consistency, this taxonomy uses "DLT system" as an all-encompassing term.

[154] 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".

[155] For example, laws in almost all states of the United States based on the Uniform Electronic Transactions Act (1999) 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".

- 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 part three of this taxonomy.
- 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 part one of this taxonomy.

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

174. Based on the analysis above, DLT systems can be regarded as providing the "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.

- The distinction between the infrastructure and application layers is echoed by an observation made by 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.[156]

C. Actors

175. 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.

[156] 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.

1. Infrastructure layer

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

- *Developer* – a person or group of persons which designs, develops and maintains the computer code that runs the system.
- *Node operator* – any person who operates a node (i.e. a computer that runs the computer code).

177. The code that runs the system may not be 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.

178. Some DLT systems also involve an *administrator* who controls:

- 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
- 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).[157]

179. A single person may be the administrator, in which case the DLT system is sometimes referred to as an "enterprise" system. The administrator role may 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 subsection D.1 under the heading "other laws" below).[158] As noted above (subsection B.2), a DLT system could be integrated into an online platform, in which case the administrator might be 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.

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

[158] 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.

180. 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

181. 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 cryptocurrencies) that are constituted or represented by data recorded in the ledger.

182. 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 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

Contract law

183. A question that commonly arises with respect to the infrastructure layer is how the DLT system is governed. As noted above (subsection B.1), 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.

184. 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. 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.[159] 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).

185. 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.

186. 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 in its legal statement on digital assets and smart contracts:[160]

> 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 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.[161]

187. 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 part one of this taxonomy.

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

[160] *Ruscoe v. Cryptopia Limited (in liquidation)*, Case No. CIV2019-409-000544, Judgment, 8 April 2020, *New Zealand Law Reports*, vol. 2020, No. 2, p. 809, [2020] NZHC 728, para. 21.

[161] "Legal Statement on Cryptoassets and Smart Contracts", November 2019, para. 30. Later 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".

Laws specific to DLT systems

188. 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.

- 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;[162]
- 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.[163]

Other laws

189. 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* in the United Kingdom.[164] In that case, a claim was brought against the core developers of several networks running the Bitcoin blockchain for breach of tortious and other extracontractual duties occasioned by a failure to take measures to allow a network participant to regain control over Bitcoin following a hack.

190. 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 towards others in the group, beyond the terms of any underlying contract between them (e.g., in the form of a partnership). However, these consequences will likely be more keenly felt in the application layer, when the DLT system is used to support off-ledger activities.

[162] Interpretation No. 12 of 2021, art. 16.

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

[164] 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); Court of Appeal, Judgment, 3 February 2023, [2023] EWCA Civ 83.

191. 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 data that are explored in part two of this taxonomy. Difficulties may arise in applying those laws on account of obstacles in identifying node operators who process the data.

Private international law

192. Given the geographic distribution of nodes and the actors involved, private international law questions regarding the infrastructure layer may arise. In particular, rules regarding the characterization of legal relationships and choice of law rules may play a significant role in determining the governance structure of a particular DLT system.

2. Application layer

193. 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 are actually used for that activity.

Contract law

194. Trade-related activities supported by DLT can involve multiple parties and an assortment of contractual arrangements. 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.

195. 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 establishes 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.

196. 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 (i) 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, (ii) how data will be fed into and recorded in the ledger, which could have implications for compliance with privacy, data localization and data security requirements, and (iii) 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.

Other laws

197. As noted above (subsection B.1), 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 part three of this taxonomy. 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.

198. Just as the infrastructure layer of DLT systems engages a range of protective laws with respect to data, 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 part four of this taxonomy will also be engaged.

E. Relevant UNCITRAL texts

1. Electronic commerce texts

199. 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.

200. 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 the concept of "integrity" under UNCITRAL electronic commerce texts:

- The 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 (article 8). 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. A similar function is prescribed in the MLIT for electronic archiving (article 19). A DLT system can be used to fulfil these functions.
- 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) of the 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. This requirement is typically fulfilled by electronic signatures that use cryptographic techniques. In a similar vein, the MLIT prescribes integrity as one of the functions of electronic seals (article 17).
- Under article 10 of the 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.

201. 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.

202. 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

203. 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 overview of the application of the MLST in these scenarios is contained in part three of this taxonomy. 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).[165]

3. Dispute resolution texts

204. As noted above (subsection B.2) DLT systems are used to support the delivery of services constituting an online platform, which could comprise dispute resolution services. An overview of the application of UNCITRAL dispute resolution texts to online dispute resolution platforms is contained in part four of this taxonomy.

4. Insolvency texts

205. An overview of the application of UNCITRAL model laws on insolvency to DLT-based digital assets is contained in part three of this taxonomy.

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

ISBN 978-92-1-002939-1

2300287

PREPRINT