



General Assembly

Distr.: Limited
30 September 2026

Original: English

**United Nations Commission on
International Trade Law**
**UNCITRAL-HCCH Joint Session on the Cross-
Border Legal Dimensions of Digital Trade**
Vienna, 9–13 November 2026

UNCITRAL's work on secured transactions involving digital assets, digital payments and digital platforms – Issues for discussion

Note by the Secretariat

Contents

	<i>Page</i>
I. Introduction.	2
II. Secured transactions involving digital assets	2
III. Digital payments.	5
IV. Digital platforms.	11



I. Introduction

1. This note presents the key legal issues being considered by UNCITRAL as part of its ongoing work on secured transactions involving digital assets (“secured transactions project”), digital payments (“digital payments project”) and digital platforms (“digital platforms project”). This note is intended to be read with [A/CN.9/S-1/2](#). As summarized in that note, these projects are at different stages of development, and thus the nature of the legal issues varies. Abbreviations and acronyms defined in [A/CN.9/S-1/2](#) are used in this note.

II. Secured transactions involving digital assets

A. Introduction

2. The secured transactions project has identified a non-exhaustive list of issues related to the use of digital assets as collateral under the MLST. Following the structure of the MLST, these issues include:

- (a) The scope and definition of digital assets, including their characterization within existing asset categories;
- (b) The creation of a security right in a digital asset;
- (c) Methods of achieving third-party effectiveness;
- (d) Priority among competing claimants;
- (e) The rights and obligations of the parties to the security agreement (i.e. the grantor and the secured creditor) and of third-party obligors;
- (f) Enforcement; and
- (g) Conflict-of-laws issues.¹

B. Scope of the project

3. The Commission mandated Working Group VI to focus on secured transactions involving “digital assets” and to assess the feasibility of extending its work to “data” at a later stage. The project thus aims to assess the extent to which the framework established by the MLST accommodates the use of ‘digital assets’ as collateral and to identify areas in which clarification, additional guidance or supplementary legislative recommendations may be desirable. Accordingly, it would be necessary to develop a working definition of the notion ‘digital asset’, which would define the actual scope of the project.

4. The MLST follows a functional, integrated and comprehensive approach to secured transactions and applies to “security rights”, defined as property rights in movable assets that are created by agreement between the grantor and secured creditor (the “parties”) to secure payment or other performance of an obligation. The scope of the MLST is defined by reference to “movable assets”, a broad and technology-neutral term that encompasses both tangible and intangible property.

5. Against that background, consideration may need to be given to whether digital assets are already covered within the existing provisions of the MLST. This may require the development of appropriate definitions and legal characterization, including an assessment of whether digital assets fall within any of the categories currently covered by the MLST or whether additional categories would need to be considered. The lack of legal clarity regarding the definition and scope of digital

¹ The term “conflict of laws” is used here (as opposed to “private international law”) as that is the term used in the MLST. In keeping with the MLST, preparatory work has focused on issues of applicable law and not on other private international law issues (e.g. jurisdiction).

assets complicates the establishment of a coherent legal framework, making it difficult to determine whether such assets would fall under existing categories of property or would require new classifications.

6. Particular questions may arise in relation to CBDCs. While CBDCs may fall within the definition of a digital asset, their legal characterization may differ from that of other digital assets because they are issued within a monetary and payment-system framework and may involve central banks, commercial banks or other intermediaries. Consideration may therefore need to be given to whether CBDCs should be treated as a distinct category of digital asset, as money, as a claim against the issuer, or as another form of intangible asset for the purposes of the MLST.

7. In light of the preparatory work, consideration could be given to the following issues:

(a) Whether digital assets can be the subject of a security right, including whether they fall under existing categories covered by the MLST;

(b) If they fall under existing categories, whether they should be listed in the definitions of such categories, for example, tangible assets (article 2(11)), intangible assets (article 2(p)), receivables (article 2(dd)), money (article 2(t)), funds credited to a bank account, negotiable instruments, non-intermediated securities (article 2(w)), or intellectual property (article 2(b));

(c) Whether the MLST should apply to outright transfer of digital assets, similar to receivables (article 1(2)); and

(d) Whether the MLST should exclude certain digital assets from its scope (article 1(3)).

8. For the time being, assets that do not fall within the scope of MLST (see article 2(3), for example, intermediated securities) are excluded from the scope of the project. This would also similarly apply to carbon credits.² As mentioned above, whether to extend the project to “data” would require a further assessment.

C. Substantive law issues

1. Creation

9. With regard to the creation of a security right in digital assets, the following issues could be addressed:

(a) Who has rights in a digital asset to grant a security right;

(b) How digital assets can be described in a security agreement;

(c) Whether a security right in digital assets would extend to proceeds (which may be a different category of asset) (article 10);

(d) Treatment of any contractual limitations by the parties on the creation of a security right in a digital asset (article 13); and

(e) Whether it is possible to create a security right in future digital assets.

2. Third-party effectiveness

10. While the primary methods of achieving third-party effectiveness under the MLST are to register a notice in the general security rights registry or to obtain possession (article 18), such methods might not be applicable to digital assets. In this regard, it may be necessary to consider other methods such as “control”. However, jurisdictions have taken different approaches to “control”, and the notion may not apply equally to all digital assets.

² *Official Records of the General Assembly, Eightieth Session, Supplement No. 17 (A/80/17)*, paras. 156 and 340–343; *Ibid.*, *Eighty-first session, Supplement No. 17 (A/81/17)*, para. 213.

11. In light of the above, the following issues could be addressed:

- (a) Methods to achieve third-party effectiveness of a security right in a digital asset, including whether the primary methods would continue to apply;
- (b) Whether to introduce “control” or other methods to achieve third-party effectiveness and if so, how to define such notions;
- (c) Whether reference should be made to asset-specific registries established for digital assets; and
- (d) Whether to expand the definition of “control agreement” to cover transactions involving digital assets.

3. Priority

12. Under the MLST, priority among competing security rights is determined generally by the order of cross or third-party effectiveness (article 29). However, there are certain asset-specific rules (articles 46 to 51).

13. With regard to digital assets, the extent to which their buyers or other transferees could acquire rights free of a security right would need to be examined (the “innocent acquirer” question). This may raise questions whether and to what extent due diligence would be required to benefit from such a rule. Similarly, the impact of the grantor’s insolvency on the priority of a security right in a digital asset would need to be examined.

14. In light of the above, the following issues could be addressed:

- (a) Whether the general priority rules would apply and if not, which other methods of third-party effectiveness should result in priority;
- (b) How to address the priority between a secured creditor and buyer or other transferees of a digital asset;
- (c) Whether the grantor’s (and possibly other related parties’) insolvency would have any impact on the priority of a security right; and
- (d) Whether it would be possible to establish an acquisition security right in a digital asset (thus, having super-priority).

4. Rights and obligations of the parties and third-party obligors

15. A wide range of new categories of parties are involved in the creation and management of, and transactions involving, a digital asset (e.g. issuer, custodians, service providers, verifying or certifying authorities and intellectual property right holders). Identifying such parties would be a first step.

16. The MLST addresses the rights and obligations of third-party obligors – namely, parties that owe obligations under the encumbered asset and their relationship with the secured creditor. Not all of the parties referred to in the previous paragraph fall under the category of “obligors”, as they are identified by their functional role in relation to a digital asset or associated legal interests. It would be useful to examine the extent to which these parties could limit the effectiveness of a security right in a digital asset, particularly during the enforcement phase.

5. Enforcement

17. While the enforcement rules under the MLST may apply generally to a digital asset, certain adaptations may be necessary. It is also anticipated that post-default rights with respect to a digital asset would be exercised mainly out-of-court. In that context, it would be necessary to consider: (i) whether a secured creditor could obtain possession of a digital asset; (ii) means available to a secured creditor to dispose of or acquire a digital asset (which may also depend on how third-party effectiveness is achieved); and (iii) valuation of a digital asset and secondary markets, including whether the enforcement could be conducted in a commercially reasonable manner.

There may be other parties involved (for example, a custodian), the interest of which would need to be protected during the enforcement phase.

6. Conflict-of-laws issues

18. The cross-border nature of a digital asset may pose challenges in applying the conflict-of-laws provision in the MLST, particularly as laws of a number of jurisdictions are intertwined. Under the MLST, the law governing the creation, third-party effectiveness, priority and enforcement of a security right depends primarily on whether the asset is tangible or intangible and the law applicable is generally either the law of the State in which the asset is located or in which the grantor is located. Against this background, participation of the HCCH in Working Group VI will be instrumental in ensuring that these complex conflict-of laws issues are comprehensively addressed.

19. With regard to digital assets, it may be difficult to determine their location, and it is also questionable whether the grantor's location should be a key factor in determining the applicable law. For example, their lack of a fixed location, cross-border nature and variety of systems to hold or transfer them can limit the relevance of location-based rules. The applicable law may instead depend on considerations such as: (i) whether and how the security right has been perfected; (ii) how digital assets are classified under the relevant laws; and (iii) whether they are held or transferred on platforms spanning multiple jurisdictions. More flexible approaches may need to be sought, including the law of the State as specified in the digital asset itself (providing for party autonomy) or in the system where the digital asset is recorded; the law of State where the issuer is located; or in the absence of such, the determination by domestic courts or other authorities based on the circumstances of the case.

III. Digital payments

A. Introduction

20. The digital payments project aims to develop technology-neutral rules, principles or standards (hereafter "rules") governing private law aspects of digital payment transactions and payment systems, particularly in the cross-border context.³

21. These rules could address a range of substantive law issues, including:

- (a) Payment finality in digital payment transactions;
- (b) Discharge of payment obligations, including the legal effects of the use of stablecoins, tokenized deposits, CBDCs and other digital assets for payment purposes (hereafter referred to generally as "digital currencies");
- (c) Rights and obligations of parties involved in digital payment transactions, including payment service providers and intermediaries;
- (d) Allocation of risks, liability and availability of remedies, including in cases of failed, delayed, erroneous or fraudulent transactions; and
- (e) Interoperability among payment systems and associated trust frameworks.

22. The scope and content of the rules have not been determined, nor has the form of an eventual text. To facilitate discussions at the Joint Session, this chapter considers the issue of scope (section B), the substantive law issues to be addressed (section C) and the possible form of the text (section D).

³ *Official Records of the General Assembly, Eighty-first Session, Supplement No. 17 (A/81/17)*, para. 205.

B. Scope

23. As noted above, the rules are expected to address:

(a) Digital payment transactions, i.e. transactions through which value is transferred, including through electronic means, between parties in the cross-border context; and

(b) Payment systems, which encompass both so-called traditional and innovative payment systems, e.g. account-based payment systems, credit transfers, debit transfers, card-based payments, mobile payments, digital wallets, platform-based payment systems, real-time payment systems and other payment infrastructures that facilitate the transfer of value by electronic means.

24. Consistent with the private law focus of the project, the rules are not expected to address regulatory matters such as banking regulation, payment system oversight, licensing, monetary policy, data privacy and protection, the protection of consumers, economic sanctions, AML/CFT requirements or financial market regulation.⁴

25. Accordingly, the Joint Session participants may wish to consider:

(a) The use of the terms “digital payment” or “electronic payment”, which have been used interchangeably thus far in the work to generally refer to the payer’s transfer of value to a payee made through electronic means;⁵

(b) A definition or description of such term;⁶ and

(c) Whether the rules should cover all payment transactions and systems including those involving digital currencies.

26. Participants may also wish to consider how the project interfaces with the CBDCs project, not only with respect to private international law issues, but also with respect to means of payment, and how the respective projects could complement one another. The same would apply to other instruments, initiatives and projects listed in [A/CN.9/S-1/2](#) (paras. 37–39).

C. Substantive law issues

27. The digital payments project identified a number of legal issues that could be suitable for treatment in a harmonized legal text. While these issues may arise in different contexts (e.g. commercial or technological), they frequently concern the same underlying legal questions, namely when a payment is final, whether the payment obligation is discharged, how risks and responsibilities should be allocated among the participants, and how interoperability can be achieved across systems and jurisdictions. This section briefly describes those issues for further consideration.

1. Payment finality

28. Payment finality concerns the determination of the point at which a payment transaction becomes legally effective, irrevocable and no longer subject to reversal. The concept performs a central function in private law because it affects legal certainty, may determine the allocation of insolvency risk and establishes the point at which parties may safely act in reliance on the receipt of funds. Divergences in

⁴ Ibid., para. 204 (noting that, inter alia, it was stressed that the work should not address regulatory matters).

⁵ [A/CN.9/1262](#), para. 4.

⁶ The Agreement on Electronic Commerce, for instance, defines the term “electronic payment” as “the payer’s transfer of a monetary claim on a person that is acceptable to the payee and made through electronic means, but does not include payment services of central banks involving settlement between financial service suppliers”. Agreement on Electronic Commerce, art. 10(1)(a), WTO, WT/MIN(26)/42 (27 April 2026).

domestic laws with respect to finality can create uncertainty and increase risks in cross-border transactions.

29. The MLICT addressed finality in the context of traditional credit transfers by linking completion of a transfer to acceptance of the payment order by the beneficiary's bank.⁷ However, modern payment arrangements employ different operating models, including those based on real-time payment infrastructure, digital wallets, intermediated payment platforms and DLT systems, in which finality may be attained differently. In some systems, value becomes available to a beneficiary before settlement between intermediaries is completed, whereas in other systems, settlement may occur automatically through transfers recorded on a distributed ledger.

30. The legal significance of a payment becoming "available" to a payee differs from the legal significance of a payment becoming "final". A payment platform may display funds as available for use even though settlement remains subject to contractual or operational conditions.⁸ Conversely, certain blockchain-based systems may render transactions technically irreversible immediately upon confirmation, notwithstanding the existence of fraud, mistake or other defects in the underlying transaction. The distinction between apparent availability of funds and legal finality may merit careful consideration.

31. Particular challenges arise in relation to payments involving digital currencies. Questions arise as to whether finality occurs when the payer initiates the transfer, when an intermediary accepts the instruction, when control over the digital currency changes, or when the transaction becomes irreversibly recorded within the relevant system. Similar issues are being considered in the HCCH work on CBDCs, particularly in relation to payment finality in cross-border digital payments.

32. In this context, Joint Session participants may wish to consider:

- (a) The legal criteria for payment finality across different jurisdictions and payment systems;
- (b) Whether payment finality should be linked to settlement, acceptance, availability of funds, transfer of control, or another legally significant event, including whether a functional and technology-neutral concept of control could assist in determining finality; and
- (d) The relationship between payment finality and payment systems involving digital currencies.

2. Discharge of payment obligations

33. Closely related to payment finality is whether and when a payment obligation has been discharged.⁹ A payment may be technically completed within a payment system while uncertainty remains regarding whether the underlying contractual obligation has been satisfied. Such uncertainty may arise when payment is made through new forms of digital money or assets, when payment is routed through complex chains of intermediaries, or where mistakes occur during execution.

34. Traditional legal frameworks generally assume payment in money issued or recognized by a State. The increasing use of digital currencies has challenged traditional assumptions regarding what constitutes payment. During exploratory work, questions were raised regarding whether transfers involving such instruments should be regarded as valid performance of contractual payment obligations and

⁷ MLICT, art. 19; see also A/CN.9/S-1/2, paras. 27 and 38.

⁸ See, e.g. United States, Court of Appeal of California, *Chen v. PayPal, Inc.*, Judgment, 2 March 2021, *California Appellate Reports, Fifth Series*, vol. 61, p. 559, available at <https://law.justia.com/cases/california/court-of-appeal/2021/a158118.html>.

⁹ The MLICT, for instance, includes in a footnote to art. 19 (Completion of credit transfer), which deals with payment finality, a suggested rule regarding discharge of an obligation of the originator to the beneficiary of the payment for States that might wish to adopt it.

whether different treatment should apply depending on the characteristics of the instrument used.¹⁰

35. Similar questions arise with respect to payment mechanisms operating through digital platforms. Commercial parties frequently rely on payment services integrated into marketplaces and other digital environments. In those circumstances, uncertainty may arise regarding whether payment is discharged when funds are transferred to the platform, credited to an account maintained by the platform, received by the ultimate beneficiary, or settled between relevant intermediaries.

36. The issue may also arise where payment is made to an authorized agent, collection service provider or payment intermediary. Domestic laws sometimes address such situations by providing that receipt by an authorized intermediary has the same legal effect as receipt by the creditor. Comparable questions may arise in digital trade environments involving payment service providers and platform operators.

37. In this context, Joint Session participants may wish to consider:

- (a) The legal effect of payment using different forms of digital payment instruments;
- (b) The circumstances in which payment to an intermediary discharges the underlying obligation;
- (c) Whether discharge should depend on finality of settlement or on another legally relevant event;
- (d) The effect of failed, reversed or incomplete payment transactions on discharge; and
- (e) The role of party autonomy in determining when discharge occurs.

3. Rights and obligations of the parties

38. Contemporary payment transactions involve an increasingly diverse range of participants, including banks, non-bank payment service providers, digital wallet providers, custodians, payment platforms, payment networks and technology service providers. As payment chains become more complex, legal uncertainty may arise regarding the respective rights and obligations of those participants.

39. The MLICT was developed for a payment environment characterized by identifiable institutions performing defined roles within a relatively linear transfer chain. By contrast, modern payment systems often involve multiple interconnected entities performing different operational functions. The allocation of responsibilities among those entities is not always transparent, particularly where functions are outsourced or distributed across several jurisdictions.

40. Questions arise regarding obligations owed by payment service providers to their users, obligations to execute payment instructions accurately and promptly, duties relating to verification and authentication, and obligations concerning security, system integrity and operational reliability. Similar questions arise regarding the obligations of users themselves, particularly in connection with correct identification of beneficiaries, safeguarding credentials and cooperation in addressing errors or fraud.

41. The growing use of smart contracts, automated payment arrangements and AI-assisted transactions further raises questions concerning attribution of actions, authority to initiate transactions and legal responsibility for decisions made with limited or no human intervention. These developments may require clarification of existing legal principles concerning consent, authorization and contractual performance.

¹⁰ A/CN.9/1262, paras. 35–36.

42. Joint Session participants may wish to consider:

- (a) Defining the principal participants in digital payment systems and their legal roles;
- (b) Rights and obligations associated with execution of payment instructions;
- (c) Obligations relating to authentication, verification and security;
- (d) Rights concerning information, notification and correction of errors; and
- (e) Issues arising from automation, smart contracts and AI-assisted payment arrangements.

4. Risk allocation, liability and redress

43. Digital payment systems distribute operational and legal risks among a wide range of participants.¹¹ Existing private law frameworks do not always provide clear answers as to who should bear losses arising from failed, delayed or erroneous transactions, nor do they consistently provide mechanisms for obtaining redress across borders.

44. In traditional payment systems, losses may arise through misdirection of funds, interruption of payment chains, insolvency of intermediaries or operational failures. Similar issues arise in instant payment systems, although they may be amplified due to compressed processing times and reduced opportunity to detect errors before execution. Fraud and verification failures have also become increasingly significant concerns.

45. Additional challenges arise in decentralized payment systems involving digital currencies. Responsibility for losses may be difficult to allocate where no single participant exercises control over the system or where transactions are executed automatically by software. Technical irreversibility can prevent correction of mistakes and may render conventional redress mechanisms ineffective. Similar questions arise where AI systems initiate or execute transactions without direct human involvement.

46. A future legal text may therefore need to consider whether common rules could be established for risk allocation and liability regardless of the underlying technology. Such rules could seek to improve predictability, ensure that losses are allocated to the participant best positioned to prevent, detect or manage the relevant risk and support the availability of redress.

47. Joint Session participants may wish to consider:

- (a) Allocation of losses resulting from delayed, failed or erroneous payment transactions;
- (b) Liability for unauthorized transactions, fraud and operational failures;
- (c) Responsibility of intermediaries and service providers;
- (d) Whether allocation of risks should differ in centralized and decentralized systems;
- (e) Availability of remedies, reversal mechanisms and redress procedures; and
- (f) Liability issues arising from automated and AI-driven payment transactions.

¹¹ During exploratory work, the rights and obligations of the parties and risk allocation, liability and redress were treated together (see [A/CN.9/1262](#), paras. 60–63) but are treated separately here for purposes of facilitating the Joint Session discussions.

5. Identity management and other interoperability challenges

48. The practical effectiveness of cross-border digital payments increasingly depends on interoperability among payment systems. While progress has been made through regional and international initiatives, fragmentation remains a significant obstacle to efficient, interoperable cross-border payment transactions and systems.

49. Fragmentation may arise from differences in payment-system rules, technical standards, digital identity frameworks, authentication methods and legal treatment of electronic records and credentials. These differences may increase transaction costs, impede straight-through processing and make it more difficult to verify parties to a payment transaction which spans across jurisdictions. They may also reduce access to payment systems, particularly for MSMEs operating internationally.

50. Digital identity was repeatedly identified during exploratory work as a critical enabler of cross-border digital payments. Payment systems depend upon reliable mechanisms for identifying participants, authenticating transactions and verifying legal authority. The MLIT may provide useful guidance regarding legal recognition and interoperability of identity management systems and trust services.

51. Exploratory work also highlighted the increasing role of globally recognized identifiers, common messaging standards and interoperable trust frameworks. Regional initiatives in Africa and Asia illustrate approaches to achieving interoperability while preserving domestic legal autonomy. These experiences suggest that future work may be able to facilitate interoperability without requiring uniformity of technology or regulation.

52. Joint Session participants may wish to consider:

- (a) Legal barriers to interoperability among payment systems;
- (b) Applicability of MLIT principles and approaches to payment systems;
- (c) Authentication and attribution of payment instructions;
- (d) Role of standardized identifiers and credentials;
- (e) Interoperability among traditional payment systems and systems involving digital currencies; and
- (f) The relationship between interoperability, party autonomy and cross-border legal certainty.

D. Possible form

53. The form of a future text on digital payments has not yet been determined. Yet, any future instrument would need to be technology-neutral, flexible and capable of application across different payment systems, payment instruments and legal traditions. In that context, Joint Session participants may wish to discuss the possible form of work, including a model law¹² (which could involve a substantial revision or modernization of the MLICT or a new model law) or other guidance texts.¹³

¹² UNCITRAL routinely develops model laws (among other techniques for legal harmonization). A model law is a legislative text that is generally prepared by a working group before being finalized and adopted by the Commission. The model law is then submitted to the General Assembly for it to recommend to States for enactment as part of their national law. A model law is generally pursued when it is expected that States will wish or need to make adjustments to the text to accommodate local requirements that vary from system to system, or where strict uniformity is not necessary or desirable.

¹³ In connection with the possibility of developing a model law, it was observed at the fifty-ninth session of the Commission that a text on digital payments could fit well together with the suite of UNCITRAL texts on electronic commerce, complement the work to support end-to-end trade digitalization and also potentially become one module of the contemplated consolidated text compiling provisions contained in existing UNCITRAL texts on electronic commerce: *Official Records of the General Assembly, Eighty-first Session, Supplement No. 17 (A/81/17)*, paras. 182–185.

IV. Digital platforms

A. Introduction

54. The Commission has requested the secretariat to develop a legal text, which would contain rules addressing substantive law issues related to the contract between the platform operator and platform user (A/CN.9/S-1/2, para. 44). This chapter advances a set of normative statements, organized according to the substantive law issues identified,¹⁴ that could serve as a basis for such rules. These statements build on existing UNCITRAL texts and suggestions put forward during exploratory work. They are presented to elicit an exchange of views on how a future text could address the platform-to-user relationship; they are not presented to initiate a drafting exercise. Joint Session participants may wish to consider generally whether corresponding rules should be included in the text, whether they are appropriately calibrated, and whether other rules could be envisaged.

B. Scope issues

55. The following rules could be developed to define the scope of the text, which is shaped by the concept of the “digital platform” (A/CN.9/S-1/2, para. 50) and the type of interactions facilitated by the platform (ibid., para. 58):

(a) The text applies to contracts under which a party (the “operator”) provides a platform service to another party (the “user”) where that service allows a user to engage in commercial activities with other users, including the conclusion of contracts for the supply of goods or services;

(b) The text governs the formation of the contract and the rights and obligations of the parties arising therefrom, but is not concerned with contract validity (cf. CISG, art. 4);

(c) The text does not affect the application laws relating to the operation of digital platforms, data privacy and protection, the protection of consumers, competition, or intellectual property (cf. MLIT, art. 2(4)).

C. Substantive law issues

1. Contract formation and modification (including incorporation of platform rules)

56. The term “platform rules” is understood to refer to the rules and policies governing the operation of the platform (including user-to-user interactions). These rules, which may be spread across multiple documents, are maintained by the platform operator and form part of its standard terms of contract.

57. Exploratory work emphasized the reliance of platform operators on standard terms in contracting with platform users (i.e. “standard-form contracting”) and the need for standard terms to be amended from time to time to keep pace with changes in the regulatory environment and technological developments, among other drivers. This translates into two contract law issues, namely (a) the enforceability of contracts of adhesion (i.e. where the platform user has no opportunity to negotiate the terms of the contract), and (b) the effectiveness of unilateral modifications to such contracts (i.e. where the platform operator changes the standard terms pursuant to a contractual discretion).

58. Standard-form contracting gives rise to concerns about power asymmetry between the parties and certainty of contract terms. Various mechanisms are employed in domestic law to address such concerns, ranging from denying the incorporation of (certain) standard terms into the contract to denying the legal effect of certain contract

¹⁴ A/CN.9/1259, para. 86.

terms.¹⁵ Such mechanisms may be grounded in general contract law or mandated by specific laws regulating digital platforms that address the platform-to-user relationship (hereafter “digital platform laws”).¹⁶

59. Standard-form contracting in international trade is not new to UNCITRAL. In fact, a specific rule on the incorporation of standard terms into international contracts for the sale of goods – which required the terms to be attached to the offer or otherwise known to the offeree – was to put forward during the preparation of the CISG; however, it was ultimately not taken up on the basis that the issue was already covered in the rules on contract formation.¹⁷ Unlike the CISG, it is not anticipated that the text will contain a comprehensive set of rules on contract formation, let alone contract validity.¹⁸ For that reason, any new rules on establishing and maintaining standard terms would need to be compatible with different approaches to these matters in domestic law.

60. The following rules could be developed:

(a) A term of the contract is not to be denied enforceability on the sole ground that it is contained in standard terms established by the platform operator;

(b) The modification of a contract is not to be denied legal effect on the sole ground that it comprises changes to the standard terms unilaterally made by the platform operator after the conclusion of the contract.

61. Such rules would be premised on contracts being formed by exchange of offer and acceptance and being modified by mere agreement of the parties (CISG, pt. II and art. 29). Formulated in a way which is familiar to UNCITRAL texts on electronic commerce (e.g. MLEC, art. 11(1)), they would enable standard-form contracting while signalling that domestic law continues to govern the enforceability of contracts of adhesion and effectiveness of unilateral modifications.

62. Additional rules on procedural aspects of standard-form contracting could be developed:

(a) The platform operator is obliged to make standard terms easily accessible to users (cf. MLIT, art. 6(d)). An obligation to publish standard terms is found in digital platform laws and is said to enhance legal certainty, transparency and predictability. A similar rule in the context of electronic contracting was considered by UNCITRAL during the preparation of the United Nations Convention on the Use of Electronic Communications in International Contract (ECC) but ultimately not taken up to avoid a duality of regimes for electronic and paper-based contracting. Nevertheless, support was expressed for an obligation to make contract terms available to encourage good business practice across business-to-business and business-to-consumer transactions;¹⁹

(b) The platform operator is obliged to give reasonable notice to the user specifying the changes to the platform rules. A similar obligation is also found in digital platform laws, which may prescribe additional procedural requirements. This rule could be supplemented by a rule that the user is entitled to terminate the contract before the changes come into effect, which was suggested during exploratory work. This supplementary rule would presumably find greater impact where the contract duration is not fixed and the user is not entitled to terminate the contract for convenience;

(c) A rule prescribing the legal consequences of non-compliance with the rule in sub-paragraph (a). Under domestic law, these consequences can range from contract avoidance to contractual or extra-contractual liability and administrative sanctions. Challenges to formulating a harmonized set out of legal consequences were

¹⁵ On the nuance between these two mechanisms, see [A/CN.9/1259](#), para. 62.

¹⁶ [A/CN.9/S-1/2](#), para. 47(a).

¹⁷ [A/CN.9/142](#), para. 278.

¹⁸ [A/CN.9/1259](#), para. 60.

¹⁹ [A/CN.9/571](#), para. 178.

foreshadowed during the preparation of the ECC.²⁰ It is worth noting that the MLIT does contain a rule establishing the liability of the service provider for loss caused due to a failure to comply with its obligations thereunder. The rule could also cover the legal consequences of non-compliance with the rule in sub-paragraph (b), noting that some digital platform laws prescribe such consequences, including denying the effectiveness or enforceability of the changes.

63. Rules on substantive aspects of standard-form contracting could also be developed, specifically on “unfair” or “unexpected” terms:

(a) The operator is not entitled to rely on a term contained in its standard terms where such reliance would be contrary to standards of good faith and fair dealing, or where the term could not reasonably be expected to be contained in the contract. Such a rule draws on case law on the CISG and UPICC article 2.1.20 on “surprising terms”;

(b) Supplementary rules could elaborate how the rule in sub-paragraph (a) would apply to terms that afford the platform operator a discretion in the performance of the contract, e.g. to change the platform rules or to restrict a user’s access to the services, which might not be “unfair” or “unexpected” on their face but in their application.

64. In various jurisdictions, laws specifically addressing unfair terms have been progressively enacted for – or extended to – business-to-business transactions. In some jurisdictions, these rules apply only to particular transactions (e.g. contracts with smaller-size enterprises or lower-value contracts). In some jurisdictions, rules are found in digital platform laws (e.g. European Union and Türkiye²¹). Further consideration of a rule on “unfair” or “unexpected” terms could benefit from a closer comparative analysis of these laws.

65. Platform-to-user contracts are commonly – but not necessarily – formed using electronic means. Existing UNCITRAL texts on electronic commerce could thus be leveraged to address the legal recognition of such contracts, including the methods relied on for users to assent to offers and for the platform rules to be incorporated into the contract. These texts are relevant not only to contract formation but also to contract performance, and could thus address the legal recognition of other matters arising in the platform-to-user relationship, including the methods relied on to identify users during the onboarding process and to achieve assurance as to the qualities of data (e.g. its origin and integrity) related to platform-based transactions.

2. Functioning of the platform

(a) Platform as a service and infrastructure

66. A digital platform is conceived as an online “service”, i.e. a service provided via the Internet or some other communications network by electronic means (sometimes called a “digital” service).²² In UNCITRAL terminology, such a service is provided through an “information system” where the service comprises the functionalities that are made available to the user (e.g. the means of communicating in electronic form) and the system comprises the infrastructure (equipment and technology) through which those functionalities are delivered. The proper functioning of a digital platform can thus be seen as a matter not only of the provision of the platform service but also of the operation of the platform system. This is not to suggest that rules on the functioning of the platform should be developed based on a particular typology of contracts (e.g. “service contract”, “works contract” or “mixed contract”), which has been cautioned against.²³ Rather, it is suggested that the rules should be

²⁰ *United Nations Convention on the Use of Electronic Communications in International Contracts* (United Nations publication, Sales No. E.07.V.2), para. 221.

²¹ Law on the Regulation of Electronic Commerce (Law No. 6563 of 23 October 2014) as amended by Law No. 7416 of 1 July 2022.

²² The platform service should not be confused with “platform as a service” (or “PaaS”), which is a type of cloud computing service.

²³ A/CN.9/1259, para. 58.

based on a clear understanding of the role played by the platform operator in its contractual relationship with the user.

(b) Obligations of both parties

67. The functioning of the platform depends on the conduct of both operator and user, which is reflected in UNCITRAL's work on the MLES and MLIT. Like digital platforms, IdM and trust services depend on confidence in the system among participants in the system, which may be promoted through minimum standards of conduct. The following rules could be developed:

(a) Both parties are obliged to observe good faith and fair dealing (UPICC, art. 1.7) in connection with the formation and performance of the contract. This obligation could be supplemented by an obligation to refrain from making false statements or misrepresentations;

(b) Each party is obliged to cooperate with the other party where reasonably expected for the other party's performance of the contract (UPICC, art. 5.1.3).

(c) Obligations of the operator

68. The operator is unlikely to define the technical specifications or underlying infrastructure of the platform in the platform rules and may only undertake to provide the platform service on an "as is" basis. As a starting point for developing rules on the operator's conduct with respect to the functioning of the platform, consideration could be given to obligations of the service provider under the MLIT and the MLES. In broad terms, these obligations fall into three categories.

69. The first category consists of obligations with respect to "operational rules, policies and practices"²⁴ (MLIT, art. 6), which could be adapted and applied to the platform operator with respect to the platform rules:

(a) The operator is obliged to maintain platform rules as appropriate to the purpose and design of the platform.

(b) The operator is obliged to make platform rules easily accessible to users. Such an obligation would overlap with the rule in para. 62(a) above. This rule could be supplemented by an obligation to disclose information on the operation of the platform.

70. A second category consists of obligations with respect to security breaches, which could be adapted to encompass breaches of the platform rules:

(a) The operator is obliged to provide means for the user to report breaches of the platform rules (cf. MLIT, art. 6(f));

(b) The operator is obliged to investigate reports (cf. MLIT, art. 7(2)(a));

(c) The operator is obliged to respond to breaches, including by suspending affected services (cf. MLIT, art. 7(2)(b)).

71. Similar obligations are said to derive from the principle of good faith and fair dealing.²⁵ The obligation to contain breaches presupposes an awareness of the breach, which could result from the operator investigating reports or monitoring the platform at its own initiative. In that regard, it is convenient to recall a suggestion that the text should not impose an obligation on the operator to monitor platform activities of users.²⁶ A rule to that effect could be developed.

²⁴ Paragraph 127 of the guide to enactment of the MLIT explains that the "operational rules" of an IdM system are "based on policies, implemented through practices and reflected in contractual agreements".

²⁵ A/CN.9/1259, para. 66(a) and (b).

²⁶ Ibid., para. 68.

72. A third category consists of obligations regarding the level of service, which could also be adapted:

(a) The operator is obliged to utilize trustworthy systems, procedures and human resources (cf. MLES, art. 9(1)(f)). This picks up a suggestion to draw on the requirement of “reliability” in UNCITRAL texts;²⁷

(b) The operator is obliged to act in accordance with the platform rules and any representations that it makes with respect to them (cf. MLIT, art. 6(c)). This obligation would be shaped by the obligation in paragraph 68(a) above;

(c) The operator is obliged to ensure the online availability and correct operation of the system (cf. MLIT, art. 6(c)).

73. It has been observed that obligations regarding the level of service also derive from the principle of good faith and fair dealing. Specifically, support has been expressed for a rule that the operator is obliged to “take reasonable care that the platform infrastructure functions as expected”.²⁸ Formulated as such, the rule evokes different approaches to the issue of conformity in the provision of services. On the one hand, the reference to “reasonable care” suggests a requirement of diligence and skill, which is commonly associated with the provision of services in various jurisdictions (cf. United Nations Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea (Rotterdam Rules), art. 14, and the duties under the “common callings” doctrine, which has been the subject of renewed interest in scholarly debate on platform liability). On the other hand, the reference to “expectations” suggests a requirement of fitness for purpose, which is commonly associated with the sale of goods (cf. CISG, art. 35(2)), but which has also been applied to the provision of software systems²⁹ and digital services.³⁰

74. A rule on conformity could be developed along either of those lines, supplemented by a rule specifying the characteristics to be assessed (e.g. quality, availability, functionality, security) and the relevant factors for such an assessment. In that regard, it is worth recalling the preference that emerged in exploratory work for applying conformity rules, as well as other obligations of the operator, to all services provided under the contract, not merely those that might be described as the “core” platform service.³¹

75. It should be noted that “due diligence” has been cited in exploratory work in a variety of contexts, including as a guiding principle and as a standard of performance. This has given rise to some uncertainty³² and may cause confusion with other legal regimes where the term “due diligence” is given a special meaning (e.g. as a condition for relying on liability shields under “safe harbour” legislation or as a procedural requirement for onboarding users).

76. Rules could also be developed on the legal consequences of a failure by the platform operator to comply with its obligations regarding the functioning of the platform. The liability of platform operators featured prominently in exploratory work, although discussions focused primarily on liability for loss caused by third parties (including other users) outside the platform-to-user contract, an issue addressed separately (para. 82 below). In practice, operators seek to limit liability in their standard terms, the effectiveness of which would depend on the role of party autonomy in the text, within the limits of mandatory law (see para. 87 below), and subject to the scope of the rule on “unfair” or “unexpected” terms (para. 63 above). As a starting point for contractual liability, a rule, inspired by the MLIT (art. 12),

²⁷ Ibid., para. 69.

²⁸ Ibid., para. 66(c).

²⁹ United Kingdom, *Bates v. Post Office Ltd.*, Judgment, 15 March 2019, [2019] EWHC 606 (QB).

³⁰ European Union, Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, *Official Journal of the European Union*, L 136 (22 May 2019), p. 1.

³¹ A/CN.9/1259, para. 73.

³² Ibid., para. 68.

could be developed that the operator is liable for loss caused to the user due to a failure to comply with its obligations under the text.

(d) Obligations of the user

77. Exploratory work has emphasized the need to strike a balance between the obligations of the parties. As a starting point, obligations of the user could be sourced from the MLIT and MLES. Specifically, obligations of the subscriber and signatory (MLIT, art. 8, MLES, art. 8, respectively) could be adapted and applied to the platform user:

(a) The user is obliged to avoid security breaches occasioned by the unauthorized access to credentials or other means used to access the platform;

(b) The user is obliged to report security breaches to the platform operator.

78. Other obligations correlating with those of the operator could also be applied:

(a) The user is obliged to use the platform in accordance with the platform rules. The legal consequences of a failure to comply with this obligation are addressed elsewhere (para. 83 below). It is not suggested to address obligations of the user regarding its platform activities on the basis that those activities would be subject to other law (e.g. laws relating to the supply of goods and services);

(b) The user is obliged to report breaches of the platform rules to the platform operator.

3. Data rights

79. The text could establish a bundle of rights and obligations of the parties with respect to data provided or “co-generated” by the user through its use of the platform (“user data”).³³ Without prejudice to requirements relating to data processing under mandatory law, including laws on data privacy and protection (see para. 55(c) above), the following rules could be developed:

(a) The operator is entitled to use or otherwise process user data for the purposes of the operation of the platform or the provision of the platform service, and to use “derived data” that is generated by such processing;³⁴

(b) The operator is obliged to provide means for the user to export user data and to erase that data at the request of the user (e.g. upon termination of the contract), subject to the rights of other users in that data;

(c) The operator is obliged to take measures to protect user data against security breaches.

4. Liability for third-party services

80. A variety of services provided by third parties may be available to users via the digital platform. These services (sometimes called “ancillary” services) may include advertising services, payment services, identity management and trust services, logistics services, fulfilment services and cloud computing services. They are provided by third parties outside the platform-to-user contract, as opposed to under it (e.g. where the operator contracts the third party to provide part of the platform services); as with platform-based transactions between users, the text would not seek to regulate the provision of services.

³³ Ibid., paras. 70–71. For an overview of “co-generated data”, see [A/CN.9/1117](#), para. 53. A similar concept of “cloud service-derived data” is addressed in *Notes on the Main Issues of Cloud Computing Contracts* (United Nations publication, 2019).

³⁴ For a definition of “derived data”, see article 10 of the draft model legislative provisions on contracts for the provision of data, the latest version of which is set out in [A/CN.9/WG.IV/WP.195](#).

81. Nevertheless, where the platform operator is involved in the selection of the third party (e.g. it requires or recommends the use of the third-party services), it has been suggested that the platform operator should be subject to due diligence obligations regarding the selection and integration of the services.³⁵ Failure to exercise due diligence in selecting third-party providers as a basis for liability has previously been discussed at UNCITRAL, notably in the context of the carriage of goods.

82. Without prejudice to restrictions under mandatory law, including competition law (see para. 55(c) above), the following rules could be developed:

(a) The operator is obliged to exercise reasonable care in selecting third-party services and in supplying the means necessary for those services to be provided through the platform. This rule could be supplemented by a clarification that the obligation is not concerned with vetting users during the onboarding process;

(b) The operator is liable for loss caused to a user due to a failure to comply with the obligation in sub-paragraph (a), provided that the user relied on the selection. This proviso is based on article 8 of the UNIDROIT Convention on International Financial Leasing. The rule could be complemented by a rule that the text does not establish an obligation to supervise the third party or otherwise render the operator liable for loss caused by the third party;

(c) The operator is obliged to disclose information on third-party services on the platform, which would supplement the obligation in para. 69(b) above;

(d) The rule on “unfair” or “unexpected” terms (para. 63 above) applies to standard terms that limit liability under other law.

5. Restricting access to the platform

83. The text could address substantive and procedural aspects of measures taken by the operator to restrict users’ access to the platform. Such matters are regulated in several digital platform laws. Exploratory work focused on the suspension or termination of the platform service for breaches of the platform rules (i.e. non-compliance with the obligation in para. 79(a) above), although an operator might seek to restrict access in other circumstances, relying on a broad contractual discretion.

84. Some reservations have been expressed about addressing this issue. Nevertheless, it does appear to be a source of contractual disputes between operators and business users who rely on digital platforms to do business, as evidenced by a growing body of case law in various jurisdictions (e.g. Brazil).

85. The following rules could be developed:

(a) The type of restriction and grounds therefor are to be specified in the contract;

(b) The operator is not entitled to impose restrictions if it does not notify the user specifying the grounds therefor;

(c) The rule on “unfair” or “unexpected” terms (para. 63 above) applies to standard terms affording the operator discretion to impose restrictions.

86. Safeguards against restrictions on access have been raised alongside termination rights of the user (see para. 62(b) above).

6. Party autonomy

87. A provision dealing with the ability of the parties to vary or derogate from the rules by agreement could be developed. The principle of party autonomy plays an important role in many of the UNCITRAL texts. However, its role in a future legal text has been questioned as it would effectively allow the platform operator to

³⁵ A/CN.9/1259, para. 74(a).

unilaterally exclude the text through its standard terms. It is also worth noting that the MLIT does not permit any derogation from provisions on the obligations and liability of service providers referenced in this chapter.

ADVANCE COPY