United Nations A/CN.9/1260

General Assembly

Distr.: General
5 May 2026

Original: English

United Nations Commission on International Trade Law
Fifty-ninth session
New York, 29 June–10 July 2026

Preparatory work on updating the Model Law on Secured Transactions

Note by the Secretariat

Contents

V.26-06266 (E) 110526 120526

I. Introduction

1. At its fifty-eighth session (Vienna, 7–23 July 2025), the Commission requested the secretariat to continue its exploratory work on secured transactions using new types of assets (A/80/17, paras. 22 (d) and 231) and to convene an expert group meeting or a colloquium to further define the scope and form of any future work in that area.

2. In response to that request, the secretariat organized a colloquium on "Harmonizing law in the age of digital trade and finance" (the "Colloquium"), which was structured in two streams, the second addressing the distinct but related topic of digital platforms and private law, on which the Commission had requested the secretariat to commence exploratory work (A/80/17, paras. 22 (e) and 266).

3. The Colloquium was held in person at United Nations Headquarters in New York from 10 to 13 February 2026 and brought together 203 participants, including representatives of Governments, international organizations, academia and the private sector. Basic information about the Colloquium was made available in document A/CN.9/1258 and related materials are available on a dedicated web page.[1]

4. This Note summarizes stream one of the Colloquium (10–11 February 2026) discussing legal issues arising from the use of digital assets as collateral in secured transactions (see chapter II). The summary of stream two of the Colloquium (12–13 February 2026) on digital platforms and private law is available in document A/CN.9/1259.

5. Chapter III of this Note outlines the outcomes of three expert group meetings held by the secretariat upon the request of the Commission. An outline of a possible text to be developed by the Commission was discussed during those meetings, which is reproduced in the annex to this Note. Chapter IV suggests a possible way forward for the Commission's consideration.

II. Colloquium on "Harmonizing law in the age of digital trade and finance – digital assets and platforms" (New York, 10–13 February 2026)

6. Stream one of the Colloquium built on the exploratory work initiated in late 2024 on the impact of new types of assets on the UNCITRAL Model Law on Secured Transactions (MLST), including a colloquium entitled "Navigating the new era of digital finance – UNCITRAL Model Law on Secured Transactions and the use of new types of assets for secured financing", which was held in New York in February 2025.[2] The report of that colloquium and the issues identified by the secretariat in document A/CN.9/1210 (paras. 15–28) informed the Commission's determination in 2025 that further preparatory work was required to assess whether concrete gaps existed that would justify clarification, guidance or updates to the Model Law (A/80/17, paras. 22(d) and 231).

7. Stream one of the Colloquium held in February 2026 consisted of seven panels, bringing together 38 speakers, and a round table discussion, that considered: (a) the extent to which the MLST could accommodate new types of assets; and (b) possible areas where further clarification or guidance might be desirable.

[1] Available at https://uncitral.un.org/en/platforms-st.

[2] See A/CN.9/1201, for a report of the Colloquium, and the relevant web page: https://uncitral.un.org/en/colloquiumsecuredtransactions2025.

A. Understanding digital assets

8. Panel 1 examined whether, and to what extent, existing secured transactions frameworks, most notably the MLST, were capable of accommodating the expanding use of digital assets in trade and finance. It was generally agreed that the functional approach of the MLST should be preserved, while its application to digital assets raised structural questions extending beyond issues of terminology or asset classification.

9. A central theme of the discussion was the increasing economic relevance of digital assets, particularly tokenized assets linked to goods, rights to payment or other assets. It was noted that tokenization was increasingly used to mobilize value embedded in operational assets, exposing frictions in legal frameworks traditionally structured around distinctions between tangible and intangible assets.

10. It was emphasized that the reference to "digital" assets often concealed the significant heterogeneity that existed among different types of assets referred to as such. A distinction was drawn between digital assets whose existence and transfer depended solely on distributed ledger technology and tokenized claims linked to issuers, custodians or underlying assets. That distinction was considered critical for secured transactions law, as it affected the operation of rules, particularly on third-party effectiveness (TPE), priority and enforcement.

11. Attention was given to the role of control. It was noted that a narrow understanding of control might undermine key policy objectives of modern secured transactions law, in particular where control was equated with possession, which could impede the grantor's continued use of such assets. This tension was described as reflecting the risk that tokenization might lead to a reliance on "possessory" security rights, which modern secured transactions regimes had departed from.

12. Against that background, the panel considered whether existing legal approaches could be adapted to preserve non-possessory security rights in digital environments. Possible approaches included separating ownership from the authority to transfer, enabling encumbrance without dispossession and recognizing technologically mediated forms of shared or conditional control, while avoiding illusory security right and excessive information asymmetries.

13. Attention was devoted to digital representations of goods, particularly negotiable documents of title in electronic form. These instruments were viewed as providing an analytical bridge between traditional secured transactions law and emerging digital practices, since their function in trade finance permitted the circulation of rights in goods without transferring possession of goods.

14. It was noted that the UNCITRAL Model Law on Electronic Transferable Records (MLETR) relied on control as a functional equivalent of possession, while deferring proprietary issues to substantive law on such transferable records. Questions therefore arose as to how such transferable records should be integrated into broader frameworks governing digital assets, including rules on innocent acquisition, TPE and conflict of laws. Reference was also made to the UNIDROIT Principles on Digital Assets and Private Law (DAPL), prepared by the International Institute for the Unification of Private Law (UNIDROIT), which reflected primarily the characteristics of digital assets.

15. Insolvency risk and custodial arrangements emerged as cross-cutting concerns. It was observed that where digital assets are held through intermediaries or platforms, the characterization of custody relationships may determine whether assets remain available to creditors upon insolvency of a custodian.

16. The absence of clear and harmonized rules on segregation, control and TPE was identified as a significant obstacle to the acceptance of digital assets as reliable collateral. On the other hand, it was noted that the pace and diversity of technological developments made the development of asset-specific regulation inadvisable.

B. Secured transaction reforms

17. Panel 2 examined secured transactions reforms from national and comparative perspectives, drawing on inputs from international organizations. It highlighted the importance of effective regimes to accommodate for new types of assets and technologically enabled credit practices.

18. Domestic experiences highlighted that secured transactions reforms extended beyond legislative reforms and required sustained institutional and technological development. The experience of Cambodia and El Salvador illustrated that the establishment of electronic collateral registries and the digitalization of secured transactions systems could enhance transparency, facilitate the use of movable assets as collateral and support access to credit. In that context, the experience of Cambodia underscored the role of a functional regime accompanied by progressive improvements to enforcement and data-sharing systems, reflecting the iterative nature of reform. The experience of El Salvador highlighted the impact of a continuously available electronic registry in broadening participation in credit markets, as evidenced by significant growth in registrations and secured lending and increased use of receivables and other intangible assets as collateral.

19. In that connection, a comparative survey of recent secured transactions reforms showed that, while many jurisdictions continued to draw on the MLST as a basis for modernization, reforms heavily reflected domestic legal traditions and institutional conditions. Deviations from the MLST were noted, including asset-specific registries and additional requirements for TPE, which were identified as potential sources of fragmentation and legal uncertainty.

20. The survey also indicated a growing trend towards legislation tailored to specific credit products, including receivables finance, factoring and warehouse receipts. It was noted that such legislation addressed particular market needs but raised concerns of fragmentation. Complementarity of asset-specific legislation and of general secured transactions regimes was emphasized.

21. As secured credit increasingly relies on dematerialized collateral, such as electronic transferable records and digital tokens, and as such assets often lack a single physical location, questions arose as to jurisdiction and applicable law. In this regard, it was emphasized that the effectiveness of security rights depended on their legal portability across borders and that private international law played a central role in ensuring coherent TPE and priority rules.

22. It was noted that control was increasingly recognized as a mechanism for establishing proprietary interests in digital assets and determining TPE and priority. Reference was made to the DAPL, which reflected the approach of the MLST with regard to certain intangibles.

23. It was observed that current reform efforts increasingly focused on the digitalization of existing collateral rather than on security right over entirely new categories of digital assets. Tokenization was described as offering potential efficiency gains, including improved record integrity and increased liquidity, but its integration into secured lending required reliable legal infrastructure and regulatory readiness. Further work was necessary to clarify the legal treatment of tokenized representations of real-world assets and the mechanisms linking digital records to underlying rights.

24. The importance of coordination among international initiatives was emphasized and it was said that any update to the MLST in relation to digital assets should be carefully coordinated with instruments and work of other intergovernmental organizations, in particular UNIDROIT and the Hague Conference on Private International Law (HCCH).

C. Possible updates to the Model Law

25. Panel 3 examined whether adjustments may be required in the MLST on the means to achieve TPE and enforcement. The discussion focused on whether the assumptions underlying the MLST remained appropriate when applied to digital assets, data and other new types of assets.

26. It was observed that many digital assets were subject to exclusive control and transfer of the assets was conducted by transferring control. The panel examined whether this aspect of digital assets being the subject of exclusive factual control warranted a differentiated treatment under the MLST. Reference was made to relevant texts developed by the International Union of Judicial Officers (UIHJ), UNIDROIT, the American Law Institute (ALI) and the European Law Institute (ELI) as well as to relevant texts being developed by the HCCH.

27. The discussion highlighted the relationship between TPE methods, such as possession and registration, and less transparent methods, such as control agreement and control. While notice registration was considered a core feature of the MLST, it was noted that a control agreement or control may better reflect the practical allocation of rights in relation to certain digital assets. It was thus discussed whether control should be introduced as a separate method of achieving TPE, without necessarily equating it to possession, and whether security right perfected by a control agreement should benefit from priority. It was noted that the absence of clear rules in this regard could increase uncertainty, particularly where multiple methods of TPE coexist.

28. These issues were further examined in the context of insolvency, where clarity as to priority and the treatment of assets is crucial. The need to preserve registration as the general method of TPE was stressed, while considering whether control-based mechanisms could be introduced for certain assets. It was noted that distinct approaches might be required for data.

29. With respect to data, questions were raised about whether the MLST could cover data – an asset that multiple parties may use simultaneously without excluding others. Reference was made to the ALI-ELI Principles for a Data Economy (ALI-ELI Principles)[3] as a starting point for treating data as an object of commercial transactions without determining its property status. It was further noted that, although the MLST's reference to "movable assets" might be broad enough to encompass data, uncertainty remained regarding what exactly constituted the subject matter of a security right in data and how exclusivity often necessary for secured lending could be achieved in practice.

30. In that context, it was discussed whether enforcement mechanisms based on taking possession and disposing of collateral could operate effectively where the collateral consists of data, given that multiple copies might exist and continued use by the grantor might not be preventable. Concerns were expressed as to whether enforcement, as currently framed, would enable a secured creditor to realize value in a predictable and commercially meaningful manner when data was provided as collateral.

31. The panel also addressed data-related receivables, understood broadly to refer to rights to payment arising from the provision, processing or licensing of data, including transactions in which data are sold, licensed or otherwise commercially exploited. The discussion focused on whether such receivables were covered by the MLST. Reference was made to the approach taken in the UNIDROIT Model Law on Factoring (MLF), which expressly includes receivables arising from such data transactions. It was noted that the absence of comparable clarification in the MLST could limit the use of data-related receivables as collateral and contribute to divergent interpretations.

[3] Accessible at https://principlesforadataeconomy.org/.

D. Control as a mechanism for third-party effectiveness and priority

32. Panel 4 considered the role of control as a basis for TPE and priority in secured transactions involving digital assets, noting both its practical relevance and its conceptual complexity. Digital assets challenged traditional perfection techniques of possession and registration, and required renewed attention to how exclusivity, publicity and priority were established in a digital environment.

33. It was observed that, under most secured transactions regimes, digital assets were treated as intangible property and relied primarily on registration for TPE. However, this approach may be insufficient for assets that are quickly transferable and difficult to locate. In that context, control was identified as offering a functional equivalent to possession, capable of supporting both TPE and enforcement, including in insolvency.

34. It was also emphasized that control should not be treated as a uniform concept; digital assets encompassed a broad range of structures, including assets whose value was intrinsic to the digital record and tokenized representations of claims or rights governed by external legal frameworks. The means by which control is exercised therefore differ, suggesting that rigid or asset-specific definitions risk over-inclusion or legal uncertainty. Accordingly, a functional notion of control focusing on the legal effects to be achieved was suggested, recognizing that a single, uniform approach may not be suitable across the diverse types of digital assets.

35. Attention was drawn to the distinction between factual and legal control.[4] In digital environments, factual control may arise from access to cryptographic credentials, protocol rules or smart contracts, and may be shared or layered among multiple actors, raising questions about exclusivity, joint exercise and the need to identify a single controller. It was noted that the MLST needed not reflect all technological arrangements in detail but must identify forms of control that reliably prevented inconsistent dispositions and justified the granting of priority.

36. While control was viewed as well suited to certain categories of digital assets, it was suggested that registration should continue to serve important publicity and transparency functions. There was support for an approach in which control and registration were complementary, and not necessarily one of them being a superior or exclusive method of perfection.

37. The discussion further emphasized the need to distinguish control over a digital token from that over rights in any underlying asset to preserving coherence with existing property, insolvency and regulatory regimes. In tokenized structures, the legal consequences of a security right continued to depend primarily on the law governing the underlying asset, and control over the token operated as a conduit rather than as an autonomous source of proprietary rights.

38. In light of those considerations, support was expressed for the development of supplementary guidance or interpretative materials clarifying the application of concepts such as control, possession and TPE in relation to digital assets in the context of the MLST.

E. Digital platforms and assets-based registries

39. Panel 5 examined the role of platform-based systems, via which digital assets are traded, in facilitating secured transactions. Particular attention was given to the role of such platforms in the creation, publicity and enforcement of security rights and the need for coherent legal approaches supporting digital trade and finance.

[4] For definitions of control see e.g.: (a) ALI-ELI Principles for a Data Economy, Data Transactions and Data Rights, Principle 3(1)(e); ELI Principles on the Use of Digital Assets as Security, 2022, p. 17; (b) MLETR, Article 11 and accompanying explanatory note, in particular, paras. 105–121; and (c) DAPL, Principles 6 and 15.

Attention was also drawn to broader legal challenges arising from platform-based activity, including the cross-border nature of platform operations, the legal characterization of platform relationships, and the role of soft law and good practices in supporting fair and predictable outcomes.

40. A central theme was the inadequacy of traditional asset classifications when applied to platform-based digital assets. Without a functional methodology for mapping such assets into MLST categories – such as receivables, negotiable instruments or other intangibles – States might classify identical assets differently, reducing cross-border certainty. A functional approach based on the economic characteristics of the assets rather than form was supported.

41. The importance of control as a basis for TPE and, where appropriate, priority was reiterated, including in relation to distributed ledger technology (DLT) models, where such models may perform functions comparable to those of a general security rights registry. For many digital assets held in platform-based systems or on distributed ledgers, system-level control – defined as the enforceable ability under system rules to block unauthorized dispositions or direct transfers – was viewed as the only practical mechanism for establishing third-party rights. For certain assets, control could operate as a primary method of perfection if supported by clear and uniform definitions.

42. Interoperability among, and clear conflict-of-laws rules for, perfection methods were thus identified as important, which included standards for reliable system operation, mechanisms for cross-registry information exchange, and neutral data models avoiding dependence on individual platforms.

43. Attention was drawn to the coexistence of general notice-based security right registries and platform-specific systems or ledgers. A distinction was made between systems producing legal effects and infrastructures supporting information sharing without creating any third-party effect. The need for interoperable architectures linking these systems was emphasized so that registry searches could reveal relevant rights. This would require governance standards for system integrity and transparency and rules on the interaction between notice registrations and system-based perfection.

44. Conflict-of-laws issues were identified as platform operations span multiple jurisdictions, including situations in which system operators, grantors, assets and creditors may all be located in different States. Without rules tailored to TPE by control or system record, lenders faced uncertainty regarding priority and enforceability. Registry interoperability was thus linked to the need for clear rules on the law applicable to system-based perfection mechanisms. Practical experience with electronic trade documentation illustrated that reliable secured transactions depended on trusted identities, verifiable records and technology-neutral functional equivalence. Digitization anchored in existing legal functions and interoperable standards were seen as capable of supporting cross-platform use of electronic trade documents, reinforcing the view that platforms operated as intermediaries while legal effect flowed from substantive law.

45. It was noted that market participants often conflate recording data on a platform with accomplishing a legal transfer or perfection. Clearer terminology distinguishing platforms, exchanges and registries was considered necessary in order to clarify when additional legal steps would be required. Digital platforms were described as operating within evolving combinations of legislation, soft-law instruments and regulatory frameworks. Non-binding recommendations on platform good practices and fair contracting standards were identified as a possible area for consideration by the Commission.

46. Overall, the importance of providing practical guidance to assist States in addressing the implications of digital assets and platform-based systems for secured transactions was emphasized (see generally document A/CN.9/1259). Such guidance was considered useful in supporting coherent national approaches and cross-border

interoperability, while avoiding overly prescriptive solutions or detailed regulation of rapidly evolving technological arrangements.

F. Enforcement and conflict of laws

47. Panel 6 examined the challenges of enforcement and conflict of laws arising from digital assets and also considered issues relating to automated enforcement in a cross-border digital environment.

48. The hybrid nature of central bank digital currencies (CBDCs), combining characteristics of currency with digital token functionality, was presented as a test case for the MLST, particularly with respect to their legal characterization and conflict of laws. It was noted that the legal treatment of CBDCs varied. Some instruments, such as the DAPL, treated CBDCs like other digital assets for private law purposes, whereas others (for example the crypto-assets regulation of the European Union [5]) excluded them recognizing their public law character. This divergence complicated the application of traditional conflict-of-laws rules applicable to money. The need to test definitions of "money" and "tangible asset" in the MLST as well as related priority and conflict-of-law provisions was emphasized.

49. It was reiterated that control as a method for TPE and priority remained a private and non-searchable mechanism, and ledger transparency did not reveal the existence of security rights (see section D above). Insolvency risks were identified where control was achieved through title transfers. For example, transferring collateral to a creditor's wallet may expose grantors and other creditors to loss or tracing difficulties if the creditor became insolvent. A complementary approach among control and registration was reiterated (see also para. 36 above).

50. The panel also examined automated and platform-executed enforcement. Modern financial systems increasingly relied on margin calls, liquidations and account freezes triggered by algorithmic rules, raising questions of attribution, legal characterization and the use of system-generated records as evidence of enforcement. Because enforcement may occur simultaneously across jurisdictions, traditional connecting factors – particularly asset location – might lose relevance. It was suggested that refinement of MLST enforcement provisions might be needed to clarify attribution of automated actions, define the legal position and duties of intermediaries and platforms executing enforcement, and avoid reliance on fictive locations for borderless digital assets.

51. In connection with those issues, the UNIDROIT Best Practices for Effective Enforcement (BPEE) were presented. The BPEE promoted predictable and efficient enforcement, including extrajudicial measures. They also provided targeted guidance on enforcement against digital assets, including circumstances in which a court order may be required. The BPEE further addressed considerations relating to automated enforcement and the exercise of remedies based on control of digital assets. The complementarity between the MLST and the BPEE was noted and welcomed, while it was stressed that differences among national enforcement regimes heighten the need for robust conflict-of-laws rules governing enforcement.

52. The panel then addressed private international law questions in more detail, comparing the traditional approach involving connecting factors with the "waterfall" approach under the DAPL (Principle 5). Under that approach, the applicable law is determined by reference to publicly accessible specifications in the digital asset or in the system on which it is recorded and, where relevant, to the statutory seat of any issuer, with the applicable law determined under the conflict-of-laws rules of the forum if no such elements are available. This flexibility allowed States to adapt rules

[5] Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 (Text with EEA relevance). Available at https://eur-lex.europa.eu/eli/reg/2023/1114/oj/eng.

to different types of digital assets while maintaining a predictable framework. It was emphasized that flexibility must be balanced with clarity to avoid increased transaction costs and cross-border uncertainty. The need to coordinate closely with the HCCH and its ongoing work on matters relevant to secured transactions and digital assets (mainly its projects on CBDCs and digital tokens) was stressed (see para. 24). In that context, calls were made that the Permanent Bureau of the HCCH could take a more active role in any future work in the area of secured transactions.

G. Other types of assets and transactions

53. Panel 7 examined other emerging types of assets and innovative secured financing structures, noting the need for secured transactions regimes to remain responsive to market developments while preserving legal certainty and supporting access to credit.

54. It was noted that tokenization was increasingly embedded in financial infrastructure, expanding the range of assets available for secured lending, including intellectual property, data-related rights and tokenized financial instruments. It was mentioned that this raised questions regarding the legal characterization of tokens, the relationship between digital records and underlying rights. The experience of Liechtenstein illustrated a legislative approach that anchored tokenized assets in private law by separating legal rights from their technological representation and treating tokens as legally relevant objects capable of embodying rights. Such approaches were described as supporting legal certainty while preserving technological neutrality. It was emphasized that clear private law characterization was essential for predictable outcomes, particularly in insolvency and cross-border contexts.

55. It was observed that intangible assets, such as intellectual property and data-related rights, accounted for an increasing share of enterprise value but remained underutilized as collateral, contributing to financing gaps. Obstacles identified included valuation uncertainty, information asymmetries, limited secondary markets, prudential capital treatment, and fragmented legal and institutional frameworks. These constraints continued to limit the effective use of economically significant intangible assets in secured lending, particularly for innovation-driven enterprises.

56. Attention was drawn to private law challenges common to intellectual property and digital assets that affected their use in secured transactions. Legal uncertainty undermined creditor confidence and market development. It was noted that digital assets might assume different legal forms, including self-hosted tokens, tokens held through intermediaries or contractual claims against platforms and assets treated as securities, which resulted in different consequences for perfection, priority and enforcement.

57. In that connection, attention was drawn to developments relating to electronic negotiable documents of title, where increasing reliance is placed on control as a functional equivalent of possession in electronic environments. These developments were seen as raising broader questions for secured transactions law concerning the classification and perfection of security rights in electronic negotiable instruments and the need for coherence across secured transactions law, transport law and negotiable documents law. Approaches identified included adapting rules applicable to negotiable documents, treating electronic negotiable documents as intangibles subject to control, or recognizing them as distinct categories of digital assets.

58. It was noted that receivables finance in digital environments was increasingly integrated within broader financial operations. The self-liquidating nature of receivables finance was described as challenging traditional distinctions between secured credit and payment flows. Functional approaches based on technologically mediated control mechanisms were identified as capable of supporting digital receivables markets across jurisdictions, alongside continued reliance on effective registries.

59. Furthermore, obstacles to cross-border financing were discussed. It was noted that restrictions on foreign lenders, limitations on guarantees, financial assistance rules, withholding taxes and certain insolvency law requirements might limit the effectiveness of secured transactions reforms even where domestic frameworks were otherwise well developed. Targeted guidance addressing such structural impediments was identified as potentially facilitating cross-border secured lending involving emerging forms of collateral.

H. Round table discussion

60. The round table considered key takeaways of the previous discussions, focusing in particular on the extent to which the MLST could accommodate digital assets and on the desirability and possible direction of future work required to ensure its continued relevance.

61. There was broad agreement that the increasing use of digital and intangible assets in financing transactions represented a structural development requiring continued attention by UNCITRAL. It was emphasized that future work should build on existing UNCITRAL instruments, maintain the functional approach of the MLST and continue to support evolving financing practices while avoiding addressing underlying substantive property law issues except where strictly necessary.

62. It was suggested that a starting point could be the preparation of explanatory material describing how the MLST applied to digital and other new types of assets (e.g. data) and identifying possible legal or practical obstacles to its effective use. Such work could clarify how the MLST operated alongside other UNCITRAL e-commerce texts and provide guidance on their coordinated use. This was considered particularly useful in light of the increasingly complex landscape of international instruments relevant to digital trade and finance and the implementation challenges faced by many jurisdictions in understanding how existing standards interact and may be implemented coherently.

63. It was also said that such work could identify legal gaps and barriers affecting transactions involving digital and other new types of assets in order to determine the scope and priorities of any further work. Attention was drawn to the importance of taking into account market practices and operational experience and consultation with industry, regulators and central banks to ensure practical relevance.

64. It was said that such preparatory work could be complemented by legislative provisions addressing issues identified in practice. Such provisions could assist States seeking to modernize their legislation, while allowing flexibility for jurisdictions at different stages of development.

65. Many participants emphasized that initial focus should be on areas of immediate practical importance, including digital assets used in trade and asset financing and the tokenization of assets linked to the real economy. In this regard, it was said that work could focus on ensuring that the MLST clearly accommodates the use of digital assets reflecting the financing practices and identifying provisions that might hinder its application.

66. The importance of coordination with other international organizations and ongoing initiatives was emphasized, with a view to ensuring consistency among international instruments and avoiding fragmentation. It was generally felt that existing work by other organizations could form a useful basis for further work.

III. Consultation with experts

67. The secretariat organized a series of expert group meetings (EGM) on this topic. One was held in person and two online. The EGM in Hong Kong, China (28 November 2025) was focused on possible revisions to the MLST, whereas the two

EGMs held online (30 March and 13 April 2026) were aimed at identifying the issues to be addressed in a text supplementing the MLST aimed at updating its application to digital assets. The draft circulated for consultations to the experts is reproduced in the annex to this Note incorporating the feedback received so far by the secretariat.

68. Experts indicated that while the MLST provided a robust foundation for secured transactions, the effective treatment of digital assets would require both guidance on the application of existing provisions and targeted revisions to address features specific to digital assets. In this regard, the experts considered whether relevant articles of the MLST adequately encompassed digital assets or would require revisions, and identified those articles potentially requiring amendment or updates to accommodate for digital assets.

69. It was widely suggested that that the guidance should be framed in a manner consistent with internationally accepted standards, market practices, and existing instruments. In addition to DAPL, references were made to the UIHJ Global Code of Digital Enforcement, the ALI-ELI Principles, the ELI Principles on the Use of Digital Assets as Security,[6] the ELI Principles and Guidance for Enforcement Against Digital Assets,[7] and work undertaken by the HCCH. However, it was generally felt that the DAPL could be a primary reference point, notably for the key notions such as control and digital assets, as they already reflect and consolidate existing international approaches.

70. The need to be adaptable to any future developments and to identify any legal gaps or inconsistencies was stressed. Issues that were deemed useful for consideration related to: (a) the different types of control of digital assets; (b) the distinction between control over a digital asset as a method of TPE and control agreements; (c) whether to also treat intermediated securities and subcustodial arrangements in the project; (d) the distinctions between a system that merely records information, a system that supports control, and a registry that creates or supports legal publicity; (e) the involvement of custodians and other actors; and (f) the interaction between secured transactions law and laws governing digital assets in general and other specific contexts.

71. Noting the importance of data as assets with economic value, experts welcomed the consideration of data as a new type of assets under MLST. However, doubts were also shared in light of several jurisdictions not acknowledging them as subject to proprietary rights. Moreover, the legal issues associated with security rights in data were said to be different from, and in many respects unrelated to, those arising in relation to digital assets. Therefore, it was felt that at a first stage, work should focus on digital assets, and should the Commission consider it appropriate, work on data could follow after some preparatory work by the secretariat, which could further reflect on the work by Working Group IV on data provision contracts.

IV. Way forward

72. In light of the above, the Commission may wish to undertake work to provide guidance to States on the application of the MLST to secured transactions involving digital assets. Such guidance could be provided regardless of whether a State has enacted the MLST, which would also offer an opportunity to further promote the adoption of the Model Law.

73. The work would build on existing international instruments (see para. 69 above) and soft law materials, in particular and where applicable, the DAPL and the BPEE.

[6] Accessible at: www.europeanlawinstitute.eu/projects-instruments/instruments/eli-principles-on-the-use-of-digital-assets-as-security/.

[7] Accessible at: www.europeanlawinstitute.eu/projects-instruments/instruments/eli-enforcement-against-digital-assets/.

Similar to how UNIDROIT prepared the MLF based on the MLST, updates to the MLST could be based on DAPL and aligned to the extent possible.

74. It is suggested that the initial focus of such work be on digital assets, which could further extend to data. While data is increasingly recognized as an asset of economic value in commercial practice, legal issues associated with security rights in data are materially different from those arising in relation to digital assets. Data is non-rivalrous, may not constitute property under many legal systems, and is frequently governed through contractual, regulatory or informational regimes rather than proprietary frameworks. For these reasons, further preparatory or exploratory work may be warranted to assess how security rights in data could be addressed within the MLST.

75. This will be without prejudice to any future consideration by the Commission. For example, the Commission may decide to embark on work involving digital assets, while requesting the secretariat to conduct further exploratory/preparatory work on data, taking into consideration the work carried out by Working Group IV on data provision contracts. Such preparatory work could assist in clarifying the legal and economic dimensions of data as a potential object of security rights and assessing whether revisions in that regard to the MLST might be warranted.

76. As to the form, work on digital assets (and possibly on data) might take the form of a text supplementing the MLST, explaining the application of MLST to digital assets and, where appropriate, making legislative recommendations. This would be similar to how UNCITRAL addressed intellectual property following the adoption of the Legislative Guide on Secured Transactions (the Supplement on Security Rights in Intellectual Property to the UNCITRAL Legislative Guide on Secured Transactions).[8] In that regard, updates to the UNCITRAL Practice Guide to the MLST might also be envisaged.

77. To advance the work, the Commission may wish to consider whether to mandate a working group to examine this topic. The secretariat could be tasked with preparing a draft text for consideration by a working group involving experts, with a session of the working group taking place in late 2026 or early 2027. Depending on the scope of the work to be mandated, it may be possible for the working group to report back to the Commission at its sixtieth session in 2027.

[8] UNCITRAL Legislative Guide on Secured Transactions: Supplement on Security Rights in Intellectual Property (2010), United Nations Publication, Sales No. E.11.V.6. Available at: https://uncitral.un.org/en/texts/securityinterests/legislativeguides/secured_transactions/supplement.

Annex

Outline of a Supplement to the Model Law on Secured Transactions

The following provides an outline of a possible structure and content of a text to supplement the MLST in its application to digital assets. For the time being, it does not address "data" or other new types of assets. It aims to identify the issues to be addressed without prejudice to the form or nature of such text.

Similar to a legislative guide, the text could comprise of a commentary, which would explain how the articles of the MLST would or might apply to digital assets by providing illustrative examples. The commentary could be followed by legislative recommendations proposing revisions to the existing articles of the MLST or new articles to be included.

Introduction

The introduction could outline the purpose, scope and structure of the Supplement and situate it in relation to the MLST and other relevant UNCITRAL texts on secured transactions.

- Key objectives and fundamental policies (legal certainty, technological neutrality, interoperability);
- Interaction between secured transactions law and other laws governing digital assets (e.g. securities regulation, AML compliance, civil procedure rules governing seizure and disclosure);
- Intended reader, including States that have not enacted the MLST and considering its implementation;
- Relationship with other UNCITRAL instruments on secured transactions and digital aspects;
- Examples of financing practices using digital and tokenized assets;
- Distinction between different types of digital assets; and
- Introduction of the notion of control without undermining non-possessory security rights in the MLST.

Chapter I. Scope of application and general provisions

Chapter I could address issues relating to the application of the MLST to digital assets, including questions of scope, definitions and the treatment of key concepts relevant to secured transactions.

- Digital assets within the scope (MLST 1);
- Applicability of existing definitions (MLST 2) and need for further clarification or new definitions (e.g. control, custodian, custody agreement, control agreement and electronic records) (DAPL *Principles 2(2), 3, 4 and 6*) – coordinated approach with other existing instruments;
- Application of MLST to outright transfers of certain digital assets (MLST art. 1(2));
- Discussion on the treatment of digital assets as proprietary rights for the purposes of secured transactions;
- Interaction between digital assets and existing MLST asset categories (receivables, securities, intellectual property (MLST 13, 16 and 17)), clarifying that security in a digital asset does not automatically result in a security right in any linked asset; and

- Treatment of tokenized representations of traditional assets, clarifying that security in a token does not automatically extend to the underlying asset which remains governed by the law applicable to that asset and the legal mechanism linking it to the token.

Chapter II. Creation of a security right

Chapter II could address how security rights in digital assets may be created, including issues relating to capacity of the grantor, asset description and tokenized assets.

- Determination of who could grant a security right in digital assets (MLST 6 and 8; reference to DAPL *Principles 3 and 14*), including where assets are held through a custodian or other intermediary as well as third parties (including issuer, administrator, or protocol-level intervention rights);
- Requirement of the grantor to establish control or to be able to transfer control over the digital assets;
- Mechanisms to allow encumbrance of digital assets while preserving the grantor's operational use of digital assets;
- Due diligence considerations relevant to the creation of a security right in digital assets (e.g. whether the grantor has the right, or authority it purports, to encumber; whether control is direct, custodial, shared or code-mediated; whether a custodian, exchange, or wallet operator holds the asset on a segregated, pooled or account-style basis);
- Description of digital assets in security agreements, including the use of technological identifiers (MLST 9; DAPL *Principles 2(5)(b) and 6*);
- Treatment of proceeds, including proceeds generated by digital assets and digital assets as proceeds of other assets (MLST 10);
- Interaction between digital assets and existing MLST asset categories (receivables, securities, intellectual property (MLST 13, 16 and 17)), clarifying that security in a digital asset does not automatically result in a security right in any linked asset; and
- Treatment of tokenized representations of traditional assets, clarifying that security in a token does not automatically extend to the underlying asset which remains governed by the law applicable to that asset and the legal mechanism linking it to the token.

Chapter III. Effectiveness of a security right against third parties

Chapter III could examine how security rights in digital assets may become effective against third parties, including the role of registration, control and their interaction.

- Applicability of existing methods of achieving TPE (notice registration or possession) to digital assets (MLST 18);
- Control (or exclusive control) as a functional equivalent of possession, or as a new method of TPE for certain categories of digital assets (reference to DAPL *Principles 6 and 15*);[1]
- Methods for establishing control for TPE purposes (DAPL *Principles 6 and 10*) and the distinction between factual and legal control;
- Relationship between registration in an asset-specific registry and control where both methods may be used – complementarity;

[1] It should be noted that where a digital record legally functions as the means of control over a payment or other right, TPE may need to be assessed at the level of the underlying right rather than solely at the level of the digital record.

- Treatment of shared, layered or multi-party control arrangements;
- Continuity and lapses in TPE where control or technological access changes;
- Use of control agreements involving custodians or wallet operators;
- Use of control agreements involving wallet operators; and
- Role and responsibilities of custodians or wallet operators in establishing TPE.

Chapter IV. The registry system

Chapter IV could discuss the operation of the MLST registry system in relation to digital assets, including its interaction with digital platforms and other asset-based systems.

- Applicability of the registry system to security rights in digital assets;
- Interoperability between the registry system and digital asset registries as well as possible distinctions (for example, some merely record information, some enable or support control, but without any publicity functions);
- Description of digital assets in registry notices, including use of technological identifiers to improve registry searchability and enable accurate identification of digital assets;
- Use of categories or classes of digital assets in notices; and
- Issues relating to the accuracy, integrity and reliability of registry information relating to digital assets.

Chapter V. Priority of a security right

Chapter V could address the application of the MLST priority rules to security rights in digital assets, including competing claims and the effects of insolvency.

- Applicability of general priority rules to digital assets (MLST 29);
- Priority where different methods of TPE are used (DAPL *Principle 16*), including identification of the relevant point in time for assessing control;
- Impact of the grantor's insolvency on priority (MLST 35);
- Priority implications when digital assets are held through custodians, wallet operators or platforms;[2]
- Priority in situations where control may be exercised by more than one person (shared) and the notion of exclusive control;[3]
- Priority among secured creditors with different control agreements;
- Rights of buyers or transferees acquiring digital assets free of security rights ("innocent acquirer" issues) (MLST 34; DAPL *Principle 8*); and
- Set-off rights of custodians or service providers against secured creditors.

Chapter VI. Rights and obligations of the parties and third parties[4]

Chapter VI could consider the respective rights and obligations of grantors, secured creditors and relevant third parties in secured transactions involving digital assets.

[2] It should be noted that the insolvency of custodians, wallet operators or platforms is generally outside the intended scope of the MLST and that any guidance should be limited to clarifying the extent of its application.

[3] It should be noted that shared or multiple control arrangements are generally treated as internal arrangements unless multiple parties each hold security rights, in which case the general priority rules apply.

[4] While the subheading of chapter VI, section II of the MLST, reads "Rights and obligations of third-party obligors", this wording should be revised as reflected in the draft outline of the Supplement for improved consistency in the context of digital assets.

Section I. Mutual rights and obligations of the parties to a security agreement

- Rights and obligations of the grantor and secured creditor regarding management and custody of digital assets;
- Duty to maintain access credentials or technological means necessary to exercise control, including the effects of loss or interruption of control; and
- Rights of the parties to obtain information regarding encumbered digital assets, particularly where such assets are held or controlled through custodial or platform-based arrangements.

Section II. Rights and obligations of third parties

- Relevant third parties in the digital asset ecosystems (DAPL *Principles 10–13*), including custodians or other service providers;
- Relevance of their legal relationship with secured creditors;
- Obligations of third parties under control arrangements, custodial structures and technological constraints; and
- Obligations of third parties to cooperate to provide information or in the context of enforcement.

Chapter VII. Enforcement of a security right (*reference to DAPL Principle 17*)

Chapter VII could examine issues relating to the enforcement of security rights in digital assets under the MLST, including automated enforcement and the role of intermediaries.

- Commercial reasonableness of enforcement involving digital assets (issues of valuation and secondary markets);
- Legal characterization and attribution of automated or algorithmic enforcement actions, including enforcement through smart contracts;[5]
- Evidentiary value of platform records during enforcement, including their potential role in demonstrating default;
- Secured creditor's ability to obtain control of the digital asset upon default (MLST 72, 76 and 77);
- Enforcement where the asset is held by a custodian or wallet operator;
- Disposal of digital assets through sale, transfer or other mechanisms (MLST 73 and 78); and
- Possibility of out-of-court enforcement (MLST 80).

Chapter VIII. Conflict of laws

Chapter VIII could address conflict-of-laws issues arising in secured transactions involving digital assets.

- Challenges in identifying the location of digital assets;
- Approach taken in the MLST with regard to tangible and intangible assets and their applicability;
- Suitability of traditional connecting factors (e.g. location of the asset or of grantor);
- Consideration of other approaches (for example, waterfall approach (see para. 52 above)) as well as other connecting factors (party autonomy; law

[5] Issues relating to smart contracts should also be flagged, without detailed discussion, also in relation to the creation of security rights and control mechanisms, as they may arise across multiple stages of secured transactions.

governing platforms, issuer or method of perfection) which could differ depending on the life cycle of the digital asset; and

- Difficulties arising from enforcement across multiple jurisdictions.

Chapter IX. Transition

Chapter IX could identify transition issues that may arise in connection with the introduction of control as a key notion governing security right over digital asset.