

ITU-T Technical Report

(06/2026)

XSTR.SR4DLTsec

**Standardization roadmap for distributed ledger
technology security**



Technical Report ITU-T XSTR.SR4DLTsec

Standardization roadmap for distributed ledger technology security

Summary

Technical Report ITU-T XSTR.SR4DLTsec provides a standardization roadmap for distributed ledger technology (DLT) security. It reviews emerging trends in DLT and related applications, and surveys existing and developing standards within ITU-T and other standards development organizations. It also includes a gap analysis identifying market needs for DLT security standardization and supporting the prioritization of future work.

Keywords

DLT security, standardization roadmap.

Note

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

© ITU 2026

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

		Page
1	Scope.....	1
2	References.....	1
3	Definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Technical Report	1
4	Abbreviations and acronyms	1
5	Emerging DLT trends and related applications	1
	5.1 Financial transactions	2
	5.2 Supply chains.....	2
	5.3 Decentralized identity and verifiable credentials	2
	5.4 Tokenization of Real-World Assets and Digital Wallets	2
	5.5 PQC and AI Integration.....	2
6	DLT security standards under development in standards development organizations.....	3
	6.1 ITU-T.....	3
	6.2 ISO TC 307.....	6
	6.3 Institute of Electrical and Electronics Engineers.....	7
	6.4 Internet Engineering Task Force	11
7	Gap analysis in DLT security standardization.....	11
8	Direction of DLT security standardization works in ITU-T.....	12
	8.1 Strategic priorities	12
	8.2 Coordination with other SDOs	12
	8.3 Roadmap update mechanism.....	13

Standardization roadmap for distributed ledger technology security

1 Scope

This Technical Report provides a standardization roadmap for distributed ledger technology (DLT) security. It addresses the following subjects:

- Emerging DLT trends and related applications that might need standardization;
- Current DLT security-related activities in ITU-T and other standards development organizations, including ISO, IEEE and IETF;
- Gap analysis on DLT security standardization;
- Direction of DLT security standardization work in ITU-T.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Technical Report

None.

4 Abbreviations and acronyms

This Technical Report uses the following abbreviations and acronyms:

AI	Artificial Intelligence
DID	DLT-based decentralized Identity
DLT	Distributed Ledger Technology
IoT	Internet of Things
PQC	Post-Quantum Cryptography
RWA	Real-World Asset
SDO	Standards Development Organization

5 Emerging DLT trends and related applications

DLT is an emerging technology that is driving innovation across various industries. As DLT-based paradigms evolve, robust standardization frameworks are needed to address associated security and privacy concerns. DLT has the potential to transform domains including financial services, supply chains, smart cities, healthcare and AI-enabled systems.

5.1 Financial transactions

DLT is increasingly adopted in financial services for cross-border payments, trade settlement and central bank digital currency (CBDC) infrastructure. Regulated stablecoins and tokenized payment instruments are developing under frameworks such as the EU MiCA regulation and emerging United States stablecoin legislation. Financial DLT deployments introduce security requirements for transaction-finality assurance, key custody under regulatory compliance obligations, and audit-trail integrity that are not fully addressed by existing general-purpose DLT security standards.

5.2 Supply chains

DLT-based supply chain solutions are being deployed for end-to-end provenance tracking, tamper-evident audit trails and automated compliance through smart contracts. Interoperability among consortium ledgers operated by different supply chain participants remains a significant challenge, requiring agreed standards for cross-ledger identity, event schemas and proof exchange. Security requirements specific to supply chain DLT, covering provenance data integrity, permissioned access control across multi-tier supplier networks and tamper-evident activity logging, remain a standardization gap.

5.3 Decentralized identity and verifiable credentials

DLT-based decentralized identity (DID) systems and verifiable credentials are gaining regulatory and market relevance: the EU eIDAS 2.0 regulation requires digital identity wallets for all member states by 2026, and the IETF SPICE Working Group is standardizing the issuer-holder-verifier credential architecture. The convergence of DID with post-quantum cryptography (PQC) requires migration of existing credential proof mechanisms to quantum-resistant signature schemes. This creates security requirements that are not yet fully addressed by existing identity-related standards, including Recommendations ITU-T X.1403, ITU-T Y.3081 and ITU-T Y.3087.

5.4 Tokenization of Real-World Assets and Digital Wallets

Institutional tokenization of real-world assets (RWAs) – equities, bonds, real estate, and carbon credits – is accelerating under the EU DLT Pilot Regime and comparable frameworks globally. Digital wallets serve as the primary custody and interaction interface for tokenized assets. Security requirements for regulated asset custody, multi-chain wallet key lifecycle management, and cross-chain wallet interoperability are not covered by existing standards, despite ITU-T TR.dw-lasf (2025) having analysed the digital wallet landscape.

5.5 PQC and AI Integration

NIST finalized the first PQC standards in August 2024, namely FIPS 203, FIPS 204 and FIPS 205, triggering migration requirements across cryptographic infrastructure. DLT systems face a specific challenge because the immutability of distributed ledgers means that quantum-vulnerable cryptographic material recorded on-chain cannot be deleted, creating a structural "harvest-now, decrypt-later" risk. In parallel, AI agents are being integrated into DLT governance and smart contract execution, introducing threat vectors including adversarial manipulation of AI-governed contracts and on-chain training data poisoning, for which dedicated DLT security standards are still limited.

6 DLT security standards under development in standards development organizations

6.1 ITU-T

Table 6-1 lists ITU-T Recommendations, Supplements and Technical Reports related to DLT in ITU-T SG13, SG20, SG21 and SG17.

Table 6-1 – ITU-T SGs Recommendations, Supplements and Technical Reports

Question/ Study group	Number	Title	Date	Security
Q14/17	X.1400 (ex X.dlt-td)	Terms and definitions for distributed ledger technology	Approved 2020-10-29	Security-relevant
Q14/17	X.1401 (ex X.sct-dlt)	Security threats of distributed ledger technology	Approved 2019-11-29	Security-focused
Q14/17	X.1402 (ex X.sra-dlt)	Security framework for distributed ledger technology	Approved 2020-07-22	Security-focused
Q14/17	X.1403 (ex X.dlt-sec)	Security guidelines for using DLT for decentralized identity management	Approved 2020-09-03	Security-focused
Q14/17	X.1404 (ex X.sa-dlt)	Security assurance for distributed ledger technology	Approved 2020-10-29	Security-focused
Q14/17	X.1405 (ex X.str-dlt)	Security threats and requirements for digital payment services based on distributed ledger technology	Approved 2021-06-29	Security-focused
Q14/17	X.1406 (ex X.stov)	Security threats to online voting system using distributed ledger technology	Approved 2021-07-14	Security-focused
Q14/17	X.1407 (ex X.srip-dlt)	Security requirements for digital integrity proofing service based on distributed ledger technology	Approved 2022-01-07	Security-focused
Q14/17	X.1408 (ex X.das-mgt)	Security threats and requirements for data access and sharing based on the distributed ledger technology	Approved 2021-10-29	Security-focused
Q14/17	TR.qs-dlt	Guidelines for Quantum-Safe DLT System	Agreed 2023-09-08	Security-focused
Q14/17	X.1409 (ex X.ss-dlt)	Security services based on distributed ledger technology	Approved 2022-07-29	Security-focused
Q14/17	X.1410 (ex X.sa-dsm)	Security architecture of data sharing management based on the distributed ledger technology	Approved 2023-03-03	Security-focused
Q14/17	X.1412 (ex X.srscm-dlt)	Security requirements for smart contract management based on the distributed ledger technology	Approved 2023-04-29	Security-focused
Q14/17	TR.dw-lasf	Technical report: Digital Wallet Landscape Analysis and Security Features	Agreed 2025-04-17	Security-focused
Q14/17	X.1400	Terms and definitions for distributed ledger technology	Approved 2026-03-16	Security-relevant

Table 6-1 – ITU-T SGs Recommendations, Supplements and Technical Reports

Question/ Study group	Number	Title	Date	Security
Q14/17	X.1413 (ex X.sc-dlt)	Security controls for distributed ledger technology	Approved 2025-05-29	Security-focused
Q14/17	X.1414 (ex X.dlt-ccs-fr)	Security requirements and framework of cross-chain service for DLT systems	Approved 2025-06-29	Security-focused
Q14/17	X.1415 (ex X.dlt-dgi)	Security requirements of distributed ledger technology (DLT) gateway for interoperability	Approved 2026-03-29	Security-focused
Q14/17	X.1417 (ex X.sr-dpts)	Security requirements for distributed ledger technology (DLT) data on permissioned DLT-based distributed power trading systems	Determined 2025-12-11	Security-focused
Q14/17	X.1418 (ex X.sg-dcs)	Security guidelines for DLT-based digital collection services	Determined 2025-12-11	Security-focused
SG13 – Future networks				
Q2/13	Y.2342	Scenarios and capability requirements of blockchain in next generation network evolution		Security-relevant
Q17/13	Y.3530	Cloud computing – Functional requirements for blockchain as a service		Security-relevant
SG13	Y.2247	Framework and Requirements of Network-oriented Data Integrity Verification Service based on Blockchain in Future Network		Security-focused
SG13	Y.3081	Self-Controlled Identity based on Blockchain: Requirements and Framework		Security-focused
SG13	Y.3087	Self-controlled identity based on blockchain – Functional requirements and architecture	2025-04-29	Security-focused
SG20 – Internet of things (IoT) and smart cities/communities				
Q3/20	Y.4476	OID-based resolution framework for transaction of distributed ledger assigned to IoT resources		Security-relevant
Q4/20	Y.4464	Framework of blockchain of things as decentralized service platform		Security-relevant
Q4/20	Y.4560	Blockchain-based data exchange and sharing for supporting Internet of things and smart cities and communities		Security-relevant

Table 6-1 – ITU-T SGs Recommendations, Supplements and Technical Reports

Question/ Study group	Number	Title	Date	Security
Q4/20	Y.4561	Blockchain-based Data Management for supporting Internet of things and smart cities and communities		Security-relevant
Q7/20	Y.4907	Reference architecture of blockchain-based unified KPI data management for smart sustainable cities		Security-irrelevant
Q3/20	Y.4486	Framework of cross edge decentralized service by using DLT and edge computing technologies for IoT devices		Security-relevant
Q4/20	Y.4508	Functional requirements and architecture of blockchain-based activity log management for Internet of things (IoT) data processing and management	2025-01	Security-focused
SG21 – Multimedia services and applications				
Q12/21	F.751.2	Reference framework for distributed ledger technologies		Security-relevant
Q12/21	F.751.5	Requirements for DLT-Based Data Management for Power Grid		Security-relevant
Q12/21	F.751.8	Technical framework for distributed ledger technology (DLT) to cope with regulation	2023-07	Security-relevant
Q12/21	F.751.16	Reference framework for distributed ledger technology (DLT) management service platforms	2024-06	Security-relevant
Q12/21	F.751.18	Framework for distributed ledger technology (DLT)-based energy metering data sharing	2024-06	Security-relevant
Q12/21	F.751.23	Framework and requirements for distributed ledger technology interoperability	2025-03	Security-relevant
Q12/21	F.751.25	Framework and requirements for distributed ledger technology-based demand response in smart grid	2025-03	Security-relevant
Q12/21	F.751.27	Framework for distributed ledger technology-based multimedia data asset service	2025-03	Security-relevant

Table 6-2 lists the on-going work items related to DLT in ITU-T.

There are five ongoing work items related to DLT security in ITU-T SG17.

Table 6-2 – Status of work items in ITU-T SG17

Question/ Study group	Acronym	Title	Timing of approval	Security
Q14/17	X.dlt-share	Security requirements for data application software based on DLT to achieve statistics	4-26	Security-focused
Q14/17	X.qsdlt-ca	Guidelines for building crypto-agility and migration for quantum-safe DLT systems	4-26	Security-focused
Q14/17	X.sr-di	Security requirements for DLT-based invoices	4-26	Security-focused
Q14/17	XSTR.gscim-dlt (ex TR.gscim-dlt)	Technical Report: Guidelines for security consideration for incident management by DLT service provider	9-26	Security-focused
Q14/17	XSTR.SR4DLTsec	Standardization roadmap for DLT security	6-26	Security-focused

6.2 ISO TC 307

Table 6-3 lists the standards and work items related to DLT security from ISO TC 307.

Table 6-3 – Standards and work items related to DLT security in ISO TC 307

Technical Committee	Number	Title	Security
JWG4	ISO/CD PAS 26348	Blockchain and distributed ledger technologies – Cybersecurity Information Sharing and Utilization Framework for the blockchain ecosystem	Security-focused
WG7	ISO/AWI PAS 26347	Interoperable protocol between digital wallets based on blockchain and DLT	Security-relevant
AHG2	ISO/AWI TR 26218	DLT and carbon markets use cases	Security-irrelevant
WG5	ISO/AWI TS 25481	Governance for DAOs in Blockchain and DLT	Security-relevant
JWG4	ISO/WD 25316	Blockchain and distributed ledger technologies – Representing non-financial digital assets using tokens	Security-relevant
WG8	ISO/DTR 25145	Blockchain and distributed ledger technology – Overview of DLT-based collections and collections management	Security-irrelevant
JWG4	ISO/WD 25126.4	Information security controls based on ISO/IEC 27002 for distributed ledger services	Security-focused
JWG4	ISO/CD 24946	Requirements and guidance for improving, preserving, and assessing the privacy capability of DLT systems	Security-focused
WG6	ISO/WD TR 24878	New and emerging DLT/Blockchain Use Cases	Security-irrelevant

Table 6-3 – Standards and work items related to DLT security in ISO TC 307

Technical Committee	Number	Title	Security
JWG4	ISO/WD 24876.6	Blockchain and distributed ledger technologies – Privacy protection when involving trust anchors in DLT-based identity management	Security-focused
WG3/JWG4	ISO/WD TS 24875-3	Smart contract security – Part 3: Holistic diagnostic method	Security-focused
WG3/JWG4	ISO/WD 24875-2.2	Smart contract security – Part 2: Code review	Security-focused
WG3/JWG4	ISO/WD 24875-1.2	Smart contract security – Part 1: Secure development	Security-focused
WG8	ISO/DPAS 24874	Guidance on the use of smart contracts in contributing to the Sustainable Development Goals (SDGs)	Security-irrelevant
WG7	ISO/DTS 23516	Blockchain and distributed ledger technology – Interoperability framework	Security-relevant
WG5	ISO/CD TS 23353.2	Blockchain and distributed ledger technologies – Auditing guidelines	Security-relevant
WG1	ISO/AWI TS 23258	Blockchain and distributed ledger technologies – Taxonomy and Ontology	Security-irrelevant
WG1	ISO/AWI 23257	Blockchain and distributed ledger technologies – Reference architecture	Security-irrelevant
JWG4	ISO/WD 23042	Reference architecture for DLT-based decentralized identity systems	Security-focused
WG1	ISO/AWI 22739	Blockchain and distributed ledger technologies – Vocabulary	Security-irrelevant
WG8	ISO/DIS 20435	A framework for representing physical assets using tokens	Security-irrelevant
WG1	ISO/DTS 18126	Taxonomy and classification for smart contracts	Security-irrelevant

6.3 Institute of Electrical and Electronics Engineers

Table 6-4 lists the standardization and work items related to DLT security from Institute of Electrical and Electronics Engineers (IEEE). Standards prefixed with "IEEE" represent approved and published standards, whereas those prefixed with "P" indicate ongoing draft standards currently under development.

Table 6-4 – Standards and work items related to DLT security in IEEE

Standards committee	Number	Title	Scope	Security
C/BDL – Blockchain and Distributed Ledgers	IEEE 3201-2024	<i>Standard for Blockchain Access Control</i>	<i>The technical framework and technical requirements of blockchain access control, including the subject, object, and access control policy of each layer of the blockchain is specified in this standard.</i>	Security-focused

Table 6-4 – Standards and work items related to DLT security in IEEE

Standards committee	Number	Title	Scope	Security
C/BDL – Blockchain and Distributed Ledgers	IEEE 3209-2023	<i>Standard for Blockchain Identity Key Management</i>	<i>IEEE Std 3209 will unite many blockchain technology providers to jointly formulate international standards for hierarchical deterministic schemes, output uniform and standardized cryptographic derivation rules between different chains, and determine multiple blockchains through mutual signature and self-certification of private keys of different chains. The same identity corresponds to the public and private keys on the chain.</i>	Security-focused
C/BDL – Blockchain and Distributed Ledgers	IEEE 3219-2023	<i>Standard for Blockchain-Based Zero-Trust Framework for the Internet of Things (IoT)</i>	<i>The surging needs for the Internet of Things (IoT) are dramatically shifting the network structure and challenging the traditional perimeter security paradigm. To establish secure and trustworthy interoperability among billions of heterogeneous interconnected devices, there is a need for standards defining a common framework. In this standard, a blockchain-based Zero-Trust access control framework is defined. The framework provides a typical implementation model and deployment variations, addressing general security and trust in IoT applications with the inspiration of the emerging Zero-Trust paradigm and blockchain technology. The leverage of blockchain and Zero-Trust discussed could provide reliable interactions among people, things, and applications in the presence of failures and attacks, and improve an IoT system's overall information technology security posture.</i>	Security-focused
C/BDL – Blockchain and Distributed Ledgers	IEEE 3205-2023	<i>Standard for Blockchain Interoperability Data Authentication and Communication Protocol</i>	<i>Blockchain interoperability is the ability of two or more blockchain systems or applications to exchange information and to mutually use the information that has been exchanged. The interfaces and protocols play a very important role in realizing interoperability. Therefore, the standard of cross-chain interoperability interfaces and protocols, especially those for data authentication and communication among homogeneous and heterogeneous blockchains systems, is needed. Such protocols coordinate blockchains while supporting multiple cross-chain models and levels to meet business demands without the need to customize gateways or exchanges for specific use cases. Provided in this standard are an infrastructure of cross-chain interoperability, as well as</i>	Security-focused

Table 6-4 – Standards and work items related to DLT security in IEEE

Standards committee	Number	Title	Scope	Security
			<i>interfaces and protocols of data authentication and communication for homogeneous and heterogeneous blockchain interoperability. The protocols include the distributed identity protocol, metadata protocol, on-chain proof transformation protocol, and cross-chain communication protocol.</i>	
C/BDL – Blockchain and Distributed Ledgers	IEEE 3250.01-2024	<i>Standard for Trusted Data Circulation based on Blockchain and Distributed Ledger Technologies (DLT)</i>	<i>The contents of this standard defines a trusted data circulation platform based on blockchain and distributed ledger technologies. The system overview of trusted data circulation platform is defined including underlying computation engine layer, blockchain and DLT core function layer, trusted data circulation layer, and interface layer. The functional modules, data circulation processes, technical and security requirements are specified. This standard includes recommendations for controlling the allowable purposes and amount of data utilization, and for data privacy and resistance to tampering during the relevant data operations.</i>	Security-focused
CTS/BSC – Blockchain Standards Committee	IEEE 3802-2022	<i>Standard for Application Technical Specification of Blockchain-based E0Commerce Transaction Evidence Collecting</i>	<i>This standard specifies the terminology, technical reference framework, basic functional requirements, and technical indicators for the application of blockchain in e-commerce transaction evidence collecting, which is the foundation of digital business interactions.</i>	Security-relevant
C/BDL – Blockchain and Distributed Ledgers	IEEE 3220.01-2025	<i>Standard for Consensus Framework for Blockchain Systems</i>	<i>The consensus framework used in blockchain technology to make the blockchain state data consistent within the distributed network environment is defined by this standard. The definition of the blockchain consensus mechanism, the protocol standard followed, the type of consensus algorithm, and the relevant scenarios are the primary focus. A practical approach for blockchain projects, which helps develop appropriate consensus mechanisms faster and more comprehensively, is also provided by the standard. Regulators and users are also provided with an authoritative reference source.</i>	Security-focused
CTS/BSC – Blockchain Standards Committee	IEEE 2140.2-2020	<i>Standard for Security Management for Customer Cryptographic Assets on</i>	<i>In this standard requirements are defined for multiple aspects of security management for customer cryptographic assets on cryptocurrency exchanges, such as user identification using multi-factor authentication, prioritized</i>	Security-focused

Table 6-4 – Standards and work items related to DLT security in IEEE

Standards committee	Number	Title	Scope	Security
		<i>Cryptocurrency Exchanges</i>	<i>protection of customer assets under unforeseen circumstances, and professional ethics of operation for cryptocurrency exchange platforms.</i>	
C/BDL – Blockchain and Distributed Ledgers	P3222.01	<i>Standard for Blockchain-based Digital Identity System Framework</i>	<i>The standard establishes requirements for blockchain based digital identity systems. The standard addresses the following attributes of the system, including but not limited to, digital identity definition, distributed digital identity creation, distributed digital identity authentication, distributed digital identity note (refers to identity credentials such as identity card, work card, member card), data or asset circulation protocols.</i>	Security-focused
(CTS/DFESC) – Consumer Technology Society/Digital Finance and Economy Standards Committee	P3847	<i>Standard for Technical Requirements and Interoperability Protocols for Decentralized Identity</i>	<i>This standard specifies technical requirements and a protocol for the implementation of interoperable decentralized identity systems. The standard focuses on the protocol for interactions between different roles (Issuer, Holder, Verifier), cryptographic verification, the format of credentials, status checks, and the use of verifiable data registries. The standard provides functional interoperability between different implementations and complements higher-level architectural frameworks. The standard addresses developers and engineers building interoperable decentralized identity components.</i>	Security-focused
CTS/MSC – Metaverse Standards Committee	P2048.201	<i>Standard for Security Specification of Blockchain-based Metaverse Accounts</i>	<i>This standard specifies the security requirements for consumer's personal accounts and public accounts of blockchain-based Metaverse technology, including general account requirements, basic security requirements, and service security requirements. This technical requirement is applicable to the management of accounts in blockchain-based metaverse.</i>	Security-focused
CTS/MSC – Metaverse Standards Committee	P2048.202	<i>Standard for Security Specifications of Blockchain-Based Metaverse Data</i>	<i>This document specifies the security requirements for data processing in the metaverse, including data transmission, data storage, data migration, data sharing, data backup and recovery, and data destruction. This document may provide a reference for the secure processing of data on the Metaverse platform.</i>	Security-focused
CTS/MSC – Metaverse	P2048.203	<i>Standard for Security Specifications of</i>	<i>This standard specifies interconnection security requirements for a blockchain-based metaverse. These requirements</i>	Security-focused

Table 6-4 – Standards and work items related to DLT security in IEEE

Standards committee	Number	Title	Scope	Security
Standards Committee		<i>Blockchain-Based Metaverse Interconnection</i>	<i>relate to the user identity, network operation, asset trading and data circulation. In improving the interoperability of metaverse platforms the standard helps to securely circulate virtual assets between different metaverse platforms.</i>	

6.4 Internet Engineering Task Force

Table 6-5 lists the standardization and work items related to DLT security from the Internet Engineering Task Force (IETF).

Table 6-5 – Standardization and work items related to DLT security in IETF

WG/RG	Title	Status	Security
SPICE WG	draft-ietf-spice-sd-cwt – SD-CWT: Selective Disclosure for CBOR Web Tokens	Under Development	Security-focused
SPICE WG	draft-ietf-spice-use-cases – SPICE Architecture: Issuer-Holder-Verifier model for digital credentials	Under Development	Security-focused
COSE WG	RFC 9679 – CBOR Object Signing and Encryption (COSE) Key Thumbprint	Published	Security-focused
JOSE/COSE WG	RFC 9864 – Fully-Specified Algorithms for JOSE and COSE	Published	Security-focused

7 Gap analysis in DLT security standardization

Table 7 below categorizes DLT security topics for which standardization is needed but is not yet fully covered. Related standards and work items are identified for each topic where applicable.

Table 7 – Gap analysis in DLT security standardization

Topic	Security issues	Priority
PQC migration for DLT (full-stack)	No standard covers end-to-end PQC migration for DLT: consensus layer key rotation, on-chain legacy cryptographic material handling, and cross-chain credential re-issuance. Existing work (TR.qs-dlt; X.qsdlt-ca) addresses partial aspects only.	H
Cross-chain unified security architecture	Trust model alignment across heterogeneous chains, atomic cross-chain transaction integrity, and relay node authentication are not standardized. Related work: X.1414; X.1415; F.751.23.	H
Security requirements for AI-DLT integrated systems	No standard addresses security of AI-governed smart contracts, on-chain AI training data integrity, adversarial inputs to DLT governance, or audit trails for autonomous on-chain decisions. Related work: X.1412 (smart contract security).	H

Table 7 – Gap analysis in DLT security standardization

Topic	Security issues	Priority
Tokenized RWA and regulated digital asset custody	Security requirements for regulated asset custody, multi-chain wallet key lifecycle management, and cross-chain wallet interoperability security are absent. Related work: TR.dw-lasf; X.1405; ISO/AWI PAS 26347.	H
DID revocation, PQC credential binding, cross-jurisdictional trust	Security requirements for DID revocation at scale, PQC-based verifiable credential signature binding, and cross-jurisdictional DID trust framework interoperability are not standardized. Related work: X.1403; Y.3081; Y.3087; IETF SPICE WG.	H
DLT incident management and forensics	Security forensics for DLT-specific incidents (consensus attacks, smart contract exploits, bridge breaches) and evidence preservation on immutable ledgers are not fully standardized. Related work: XSTR.gscim-dlt (draft).	M

8 Direction of DLT security standardization works in ITU-T

Based on the trend analysis in clause 5, the standards development organization (SDO) standards survey in clause 6, and the gap analysis in clause 7, this clause identifies strategic directions for ITU-T DLT security standardization work.

8.1 Strategic priorities

The following areas are identified as strategic priorities for new ITU-T standardization work, reflecting the gaps identified in clause 7 and the deployment urgency described in clause 5.

First, a new Recommendation addressing end-to-end PQC migration for DLT systems should be initiated as a high-priority item, complementing the existing TR.qs-dlt and the forthcoming X.qsdlt-ca. The new work item should specifically address consensus layer key rotation procedures, handling of immutable on-chain legacy credentials, and coordinated cross-chain re-issuance during cryptographic migration.

Second, a security requirements Recommendation for AI-DLT integrated systems should be considered to address the security of AI-governed smart contracts, on-chain AI training data integrity, and audit-trail requirements for autonomous on-chain decisions. This area has limited coverage in current SDO work and is of high urgency given the rapid deployment of AI agents in decentralized finance and on-chain governance.

Third, security requirements for tokenized regulated asset custody and multi-chain digital wallet key management should be developed, building on TR.dw-lasf and coordinating with ISO/TC 307/WG7 work on digital wallet interoperability.

8.2 Coordination with other SDOs

ITU-T SG17 Q14/17 should maintain active coordination with ISO/TC 307/JWG4 on security controls and privacy (ISO/WD 25126.4; ISO/CD 24946), with IETF SPICE WG on credential architecture (SD-CWT; IHV model), and with NIST on PQC algorithm migration timelines. Liaison documents should be exchanged to avoid normative conflicts between ITU-T X-series DLT security Recommendations and parallel ISO/IEEE work items in the identity and cross-chain security domains.

8.3 Roadmap update mechanism

XSTR.SR4DLTsec should be reviewed and updated periodically during the study period. Updates should reflect: (a) newly approved, agreed or determined Recommendations and Technical Reports; (b) changes in the SDO landscape identified through liaison; and (c) evolution of technical trends that affect standardization priorities. The gap analysis table in clause 7 and the priority assignments in clause 8.1 should be primary revision targets during each update cycle.
