ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T F.751.8 (07/2023)

SERIES F: Non-telephone telecommunication services

Multimedia services

Technical framework for distributed ledger technology (DLT) to cope with regulation

ITU-T F-SERIES RECOMMENDATIONS

Non-telephone telecommunication services

TELEGRAPH SERVICE	F.1-F.109
Operating methods for the international public telegram service	F.1-F.19
The gentex network	F.20-F.29
Message switching	F.30-F.39
The international telemessage service	F.40-F.58
The international telex service	F.59-F.89
Statistics and publications on international telegraph services	F.90-F.99
Scheduled and leased communication services	F.100-F.104
Phototelegraph service	F.105-F.109
MOBILE SERVICE	F.110-F.159
Mobile services and multidestination satellite services	F.110-F.159
TELEMATIC SERVICES	F.160-F.399
Public facsimile service	F.160-F.199
Teletex service	F.200-F.299
Videotex service	F.300-F.349
General provisions for telematic services	F.350-F.399
MESSAGE HANDLING SERVICES	F.400-F.499
DIRECTORY SERVICES	F.500-F.549
DOCUMENT COMMUNICATION	F.550-F.599
Document communication	F.550-F.579
Programming communication interfaces	F.580-F.599
DATA TRANSMISSION SERVICES	F.600-F.699
MULTIMEDIA SERVICES	**F.700-F.799**
ISDN SERVICES	F.800-F.849
UNIVERSAL PERSONAL TELECOMMUNICATION	F.850-F.899
ACCESSIBILITY AND HUMAN FACTORS	F.900-F.999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T F.751.8

Technical framework for distributed ledger technology (DLT) to cope with regulation

Summary

Recommendation ITU-T F.751.8 defines the technical framework for distributed ledger technology (DLT) to cope with regulation, including regulatory challenges and technical capacities. The design of the technical framework of DLT in this Recommendation is closely related to DLT properties including decentralization, immutability and openness. This Recommendation can be used as guidance for the DLT system when facing regulation for DLT service providers and DLT system developers.

History [*]

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T F.751.8	2023-07-10	16	11.1002/1000/15174

Keywords

Blockchain, distributed ledger technology, regulation.

[*] To access the Recommendation, type the URL https://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

© ITU 2023

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

Recommendation ITU-T F.751.8

Technical framework for distributed ledger technology (DLT) to cope with regulation

1 Scope

This Recommendation defines a technical framework for distributed ledger technology (DLT) to address regulation. The scope of this Recommendation includes:

– The regulatory challenges related to DLT;

– The technical capacities for DLT to cope with regulation.

The target users of this Recommendation are DLT service providers and DLT system developers. DLT regulators are not target users. The objective of this Recommendation is not to provide regulatory solutions for DLT regulators, but rather to propose technical solutions to challenges related to DLT regulations.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T F.751.0]	Recommendation ITU-T F.751.0 (2020), *Requirements for Distributed Ledger Systems*.
[ITU-T X.1401]	Recommendation ITU-T X.1401 (2019), *Security threats of distributed ledger technology*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 consensus [b-ITU-T X.1400]: Agreement that a set of transactions is valid.

3.1.2 consensus mechanism [b-ITU-T X.1400]: Rules and procedures by which consensus is reached.

3.1.3 distributed ledger [b-ITU-T X.1400]: A type of ledger that is shared, replicated, and synchronized in a distributed and decentralized manner.

3.1.4 privacy [b-ITU-T J.160]: A way to ensure that information is not disclosed to anyone other than the intended parties. Information is usually encrypted to provide confidentiality. Also known as "confidentiality".

3.1.5 threat [b-ISO/IEC 27000]: Potential cause of an unwanted incident, which may result in harm to a system or organization.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AML	Anti-Money-laundering
DLT	Distributed Ledger Technology
FATF	Financial Action Task Force on money laundering
IoT	Internet of Things
KYC	Know Your Customer
PKI	Public Key Infrastructure
TEE	Trusted Execution Environment

5 Conventions

This Recommendation uses the following conventions:

– The keyword "**is required to**" and "shall" indicate a requirement that must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

– The keywords "**is recommended**" indicate a requirement that is recommended but which is not absolutely required. Thus, this requirement needs not be present to claim conformance.

– The keywords "**can optionally**" and "**may**" indicate an optional requirement that is permissible, without implying any sense of being recommended. These terms are not intended to imply that the vendor's implementation must provide the option, and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Overview

Distributed ledger technology (DLT) enables large groups of nodes in the distributed ledger network to reach agreements and record information without a central authority. The fast development of DLT brings challenges for regulation including privacy/confidentiality protection, data protection regulation, network attack handling and cryptocurrency regulation, among others. DLT has been applied to various domains such as cryptocurrency, supply chain management and IoT. Thus, it is necessary to summarize regulation requirements based on the analysis of DLT functions and properties and define the technical framework to fill the gap between openness and regulation. Precursor work was done in [b-DLT 4.1] and evolved in technical specifications found hereinafter.

7 Regulatory challenges

7.1 Leakage of confidential information

Confidential information might be leaked directly on-chain, by combining external data with on-chain or off-chain data. Transactions and public keys might be directly available on-chain, particularly with permissionless DLT systems. External data might allow the identification of public keys with persons or companies and thereby identify transactions.

In permissionless distributed ledgers, there is no access control and all data directly stored on-chain is accessible to everybody. Storing (unencrypted) confidential data on a permissionless distributed ledger is considered leakage of confidential data.

7.2 Immutability of records and absence of functionality to erase transactions/contents

Depending on the DLT application and type of data, regulations require the erasure of personal data. This requirement is contained in laws and regulation, which can create conflicts with the immutability of DLT systems.

NOTE – The "right to be forgotten" in Art. 17 of the EU General Data Protection Regulation ([b-GDPR]) is an example of the requirement of data erasure.

Data protection regulation and other laws might also require correcting transactions. This is only possible through forks that put the reliability of distributed ledger systems at risk.

7.3 Security threats

The security threats to DLT components refer to clauses 5.1 (threats to protocols), 5.2 (threats to networks) and 5.3 (threats to data) of [ITU-T X.1401].

7.4 Loss of tokens, digital currency and other assets

The loss of tokens, digital currency and other assets often result from threats to data. However, these losses might also be caused by wilful deceit regarding fraudulent coins, fraudulent distributed ledger systems or the entity behind account addresses. Phishing attacks might also trick people into making transactions they would not otherwise make.

7.5 Financial and other crimes

Distributed ledger systems can be used for financial crimes such as money laundering or to facilitate other crimes such as ransomware attacks, among others. Transactions might contain illegal contents that obey the rules of the protocol but are in conflict with regulations and other laws.

8 Technical capacities to cope with regulation

8.1 Technical framework

The design of the technical framework of DLT to cope with regulation is closely related to DLT properties including decentralization, autonomy, immutability, openness, transparency and anonymity. DLT technical capacities to cope with regulation are defined from the following aspects: application level, privacy/confidentiality, data erasure, data security and base level. In permissioned DLT, accountability is critical and DLT service providers are recommended to define an underlying orchestration legal entity to reduce the uncertainty of the regulatory actions.

8.2 Application level capacities

- DLT systems that are used to transfer digital assets are recommended to include a module that supports FATF-rules and/or specific national regulations.
- It is recommended in permissioned DLT to support know your customer (KYC) and anti-money-laundering (AML) functionalities by using techniques such as public key infrastructure (PKI) based signatures.
- DLT service providers and system developers can optionally use techniques such as limiting the rights of transactions and block accounts to intervene in transactions created by malicious and abnormal nodes.
- DLT service providers and system developers can optionally provide a link to officially recognized PKI. This can optionally be used to identify transactions with a legal entity.

8.3 Privacy/Confidentiality capacities

- A DLT system is recommended not to publish confidential information or personal data including account identity information, personal data/personal identifiable information, transaction data, digital assets information and other confidential information unless there is a justification for publishing it.

- It is not recommended to store data containing this type of information on a permissionless DLT system. If this type of information needs to be verified by a DLT system, it is recommended to only store a commitment or other proof of the data on the DLT system.
- If it cannot be avoided to store the data on a DLT system, it is recommended to use cryptographic methods such as zero knowledge proofs, account confusion or methods based on hardware isolation (i.e., TEE) to protect confidential data (business data or personal data) from disclosure.
- It is recommended to properly secure confidential data stored off-chain by some appropriate cryptographic methods.
- DLT systems in which confidential information is stored are recommended to offer appropriate access control to ensure that only authorized access is possible. The access is recommended to be limited to those who are authorized and/or to situations where access is authorized.
- Off-chain storage is recommended to use the appropriate access control methods.
- Encryption, zero knowledge proofs and cryptographic hash-functions can optionally be used to secure information on-chain. However, immutable on-chain storage faces the challenge that compromised access methods cannot be blocked. It is recommended to perform a risk analysis and/or data protection impact analysis regarding on-chain storage of confidential/personal data.

8.4 Data erasure capacities

A high level of immutability is a key property of distributed ledger systems. Removing immutability completely would therefore often remove the reason why a distributed ledger system is chosen in the first place.

When immutability is not desired for all attributes of a transaction, it is recommended to store data off-chain and only validate it, for example, by storing a proof to validate the off-chain data. For this purpose, technologies such as zero knowledge proofs, a commitment of the data or a hash-value can optionally be stored on-chain. Appropriate care is required to be taken that no undesired information can be derived from the data stored on-chain.

In some use cases, verification of off-chain data might not be enough, and data persistence is needed. Still, the persistence of data might only be required for a specific period of time or while some conditions are met. Examples for such use cases are transaction data that needs to be preserved only as long as no following transaction exists, and records that need to be preserved for a specific time period (e.g., 10 years). In these cases, a distributed ledger can optionally be built that automatically removes this data when the following transaction has been completed or the time period has passed. Techniques such as pruning [b-Nakamoto] and chameleon hashes [b-Camenisch] can optionally be used.

When such technologies are used

- It shall be clearly defined what parts of the ledger shall remain immutable;
- It shall be clearly defined under which conditions other parts can be changed;
- The protocol of the distributed ledger shall define how this data is to be erased;
- The protocol of the distributed ledger shall ensure that data which is required not to be erased or modified is still protected against modification;
- It shall be ensured that archive copies of the ledger shall only be held according to applicable regulation.

The objective of data erasure is to respond to regulation requests by local laws, recommendations or other requirements. The erasure functionality is recommended to be limited to some part of the data so that trust in the immutability of the rest of the data is maintained.

8.5 Data security capacities

– DLT service providers and system developers are recommended to ensure that the design of DLT systems using cryptography and other technologies meets the security and performance requirements of DLT services, including reliability, completeness and immutability particularly by using appropriate cryptographic algorithms and consensus mechanisms.

– DLT service providers and system developers are recommended to ensure the consistency of data on-chain.

8.6 Base level capacities

– DLT service providers and system developers are recommended to employ appropriate care to ensure the integrity, confidentiality, enforceability, availability and usage of DLT networks.

– DLT system developers are recommended to counter network threats with an appropriate security framework.

– DLT service providers and system developers can optionally use methods such as expanding computing power or stake resources to prevent consensus attacks.

– DLT service providers and system developers are recommended to support the security of smart contracts running on DLT systems by formal verification or other vulnerabilities detection methods.

– DLT system developers can optionally design fault-tolerance in DLT systems against malicious nodes. The DLT system is recommended to recover when a set of normal nodes are malfunctioning or become malicious nodes.

Bibliography

[b-ITU-T J.160] Recommendation ITU-T J.160 (2005), *Architectural framework for the delivery of time-critical services over cable television networks using cable modems*.

[b-ITU-T X.1400] Recommendation ITU-T X.1400 (2020), *Terms and definitions for distributed ledger technology*.

[b-Camenisch] Camenisch J., Derler D., Kernn S., Pöhls H. C., Samelin K., and Slamanig D. (2017), *Chameleon-hashes with ephemeral trapdoors and Applications to Invisible Sanitizable Signatures*, Public-Key Cryptography , Berlin, Springer, pp. 152–182. https://doi.org/10.1007/978-3-662-54388-7_6.

[b-DIN SPEC 4997] DIN SPEC 4997 (2020), *Privacy by blockchain design: A standardised model for processing personal data using blockchain technology*.

[b-DLT 4.1] ITU-T HSTP.DLT-RF (2019), *Distributed ledger technologies: Regulatory framework.*

[b-GDPR] European Union General Data Protection Regulation law, Article 17, *Right to erasure ('right to be forgotten'),* https://gdpr.eu/article-17-right-to-be-forgotten/.

[b-ISO/IEC 27000] ISO/IEC 27000:2016, *Information technology – Security techniques – Information security management systems – Overview and vocabulary.*

[b-Nakamoto] Nakamoto S. (2008), *Bitcoin: A Peer-to-Peer Electronic Cash System.* https://bitcoin.org/bitcoin.pdf.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	**Non-telephone telecommunication services**
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Published in Switzerland
Geneva, 2023