



INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

F.751.2

(08/2020)

SERIES F: NON-TELEPHONE TELECOMMUNICATION
SERVICES

Multimedia services

Reference framework for distributed ledger technologies

CAUTION !

PREPUBLISHED RECOMMENDATION

This prepublication is an unedited version of a recently approved Recommendation. It will be replaced by the published version after editing. Therefore, there will be differences between this prepublication and the published version.

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/had not] received notice of intellectual property, protected by patents, 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 TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2020

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

New Recommendation ITU-T F.751.2 (ex H.DLT)

Reference framework for distributed ledger technologies

Summary

This Recommendation defines the reference architecture for distributed ledger technology (DLT), the hierarchical relationship and specific functions of the DLT architecture, important modules and specific functions in the structure of DLT, the main technical route and direction of the core module in the DLT. It can be used as a guideline for DLT service providers to build system, and for the organizations to select and use a DLT platform.

Keywords

DLT; distributed ledger technology; ledger; blockchain; reference architecture; architecture; components; functions; platforms

CONTENTS

	Page
1 Scope.....	4
2 References.....	4
3 Definitions	4
3.1 Terms defined elsewhere	4
3.2 Terms defined in this Recommendation	5
4 Abbreviations and acronyms	5
5 Conventions	6
6 Architecture Overview.....	6
6.1 Overview.....	6
6.2 Resource and infrastructure functions	7
6.3 Protocol / governance and compliance functions	7
6.3.1 Consensus mechanism functions.....	8
6.3.2 Ledger management functions	8
6.4 Application functions.....	8
6.4.1 Smart contract mechanism functions	8
6.4.2 DApp management functions.....	8
6.5 Operation and maintenance functions	9
6.6 External interaction management functions	9
6.7 Extension functions	9
6.7.1 Internal system extensions.....	9
6.7.2 External system extensions	9
7 Functional Components	9
7.1 Core layer.....	10
7.1.1 Network and infrastructure.....	11
7.1.2 Extendable protocol communication	11
7.1.3 Network (P2P network) management	11
7.1.4 Storage service	12
7.1.5 Consensus mechanism.....	12
7.1.6 Smart contract mechanism	13
7.1.7 Ledger.....	15
7.1.8 Data integrity and trusted storage.....	15
7.1.9 Account management	16
7.1.10 System management.....	16
7.1.11 Utility.....	16
7.2 Service layer	17

	Page
7.2.1 Expandable services for account management.....	17
7.2.2 Expandable services for system management	18
7.2.3 Expandable services for smart contract mechanism.....	18
7.2.4 Expandable services for data integrity	18
7.2.5 Trust endorsement management.....	18
7.3 Application service platform	19
7.3.1 DApp service interfaces	19
7.3.2 Accounting, authorization and authentication.....	19
7.3.3 Data privacy	20
7.3.4 Data storage and synchronization.....	20
7.4 DLT applications	20
7.5 DLT extendable interfaces and external services	20
7.5.1 Administration interfaces	20
7.5.2 External governance interfaces	20
7.5.3 Exchange protocol and extensional resources.....	20
Bibliography.....	22

List of Figures

	Page
Figure 1 – High-level conceptual architecture of DLT	7
Figure 2 – Architecture diagram	10
Figure 3 – Two options of Typical flow of DLT systems.....	10

New Recommendation ITU-T F.751.2

Reference framework for distributed ledger technologies

1 Scope

This Recommendation defines the reference architecture for distributed ledger technology (DLT), the hierarchical relationship and specific functions of the DLT architecture, important modules and specific functions in the structure of DLT, the main technical route and direction of the core module in the DLT.

It can be used as a guideline for DLT service providers to build system, and for the organizations to select and use a DLT platform.

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; all 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.

[ITU-T F.751.0] ITU-T Recommendation F.751.0 (2020), *Requirements for distributed ledger systems*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 address [ITU-T F.751.0]: Identifier for one or more entities performing transactions or other actions in a blockchain or distributed ledger network.

3.1.2 asset [ITU-T F.751.0]: An asset is representation of value. It can be a diamond, a unit of currency, items inside a shipping container, etc. An asset can be physical or virtual.

3.1.3 blockchain [ITU-T F.751.0]: A type of distributed ledger which is composed of digitally recorded data arranged as a successively growing chain of blocks with each block cryptographically linked and hardened against tampering and revision.

3.1.4 consensus [ITU-T F.751.0]: Agreement that a set of transactions is valid.

3.1.5 entity [ITU-T F.751.0]: Entity refers to something that exist as a human, an organization, a smart contract, or a device. An entity uses DLT to solve the problem of its business or information systems.

3.1.6 ledger [ITU-T F.751.0]: Information store that keeps final and definitive (immutable) records of transactions.

3.1.7 node [ITU-T F.751.0]: Device or process that participates in a distributed ledger network.

3.1.8 permissionless DLT [ITU-T F.751.0]: Distributed ledger system where permissions are not required to maintain and operate a node.

3.1.9 public DLT [ITU-T F.751.0]: A public DLT has transaction records that are readable by anyone.

3.1.10 private DLT [ITU-T F.751.0]: A private DLT limits the transaction records read access to some authorized groups.

3.1.11 smart contract [ITU-T F.751.0]: Program written on the distributed ledger system which encodes the rules for specific types of distributed ledger system transactions in a way that is recommended to be validated and triggered by specific conditions.

3.1.12 Token [ITU-T F.751.0]: a digital representation of value on a shared distributed ledger that is owned and secured using cryptography to ensure its authenticity and prevent modification or tampering without the owner's consent.

3.1.13 Transaction [ITU-T F.751.0]: An incident or an operation which lead the status of ledger changed, such as adding a record to the ledger, equivalent exchange based on currency, etc.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 event model: Model where consensus takes place upon event.

3.2.2 state model: Model where consensus takes place upon state.

3.2.3 UTXO model: Model where transaction spends output from prior unspent transactions and generates new outputs that can be spent in the future. The unspent transactions are kept in each node.

3.2.4 balance model: Model that keeps track of the balance of each account as a global state. The balance of an account is checked to make sure it is larger than or equal to the spending transaction amount.

3.2.5 trust endorsement: An endorsement for entities inside DLT systems to trust each other, e.g., for one node to trust other nodes. E.g., the endorsement can be a programmable governance model, or contracts or agreements signed by node owners.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AAA	Authentication, Authorization and Accounting
AES	Advanced Encryption Standard
API	Application Programming Interface
BFT	Byzantine Fault Tolerance Algorithm
CA	Certificate Authority
dBFT	Delegated Byzantine Fault Tolerance Algorithm
DApp	Decentralized Application
DES	Data Encryption Standard
DID	Decentralized Identity
DLT	Distributed Ledger Technology
DPoS	Delegated Proof of Stake
ECC	Elliptic Curves Cryptography
EVM	Ethereum Virtual Machine
IBE	Identity Based Encryption
JVM	Java Virtual Machine
KYC	Know Your Customer
P2P	Peer to Peer

PKI	Public Key Infrastructure
PoS	Proof of Stake
PoW	Proof of Work
RPC	Remote Procedure Call
SDK	Software Development Kit
SHA	Secure Hash Algorithm
SM3	Shang Mi 3 (One of the hash algorithms specified in [b-ISO/IEC 10118-3])
TEE	Trust Execution Environment
TXO	Transaction Output
UTXO	Unspent Transaction Output
VBFT	Byzantine Fault Tolerance with Verifiable Randomness
VM	Virtual Machine

5 Conventions

In this Recommendation:

- The keywords "is required to" indicate a requirement which 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 which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.
- The keywords "can optionally" indicates an optional requirement which is permissible, without implying any sense of being recommended. This term is 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 this Recommendation.

6 Architecture Overview

6.1 Overview

The high-level architecture constrains the highly abstract hierarchical architecture of distributed ledgers. The high-level architecture can cover almost all distributed ledgers, including public chains represented by Ethereum [[b-ethe](#)] and Bitcoin [[b-bitc](#)], private chains represented by Hyperledger Fabric and non-blockchain distributed ledgers systems.