International Telecommunication Union

ITU-T Technical Specification

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(1 AUG 2019)

ITU-T Focus Group on Application of
Distributed Ledger Technology
(FG DLT)

Technical Specification FG DLT D1.1

Distributed ledger technology terms and definitions

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 procedures for establishment of focus groups are defined in Recommendation ITU-T A.7.

Deliverables of focus groups can take the form of technical reports, specifications, etc., and aim to provide material for consideration by the parent group in its standardization activities. Deliverables of focus groups are not ITU-T Recommendations.

The ITU Telecommunication Standardization Advisory Group established the ITU-T Focus Group on Application of Distributed Ledger Technology (FG DLT) in May 2017.

FG DLT concluded and adopted its Deliverables on 1 August 2019.

Type	**Number**	**Title**
Technical Specification	FG DLT D1.1	DLT terms and definitions
Technical Report	FG DLT D1.2	DLT overview, concepts, ecosystem
Technical Report	FG DLT D1.3	DLT standardization landscape
Technical Report	FG DLT D2.1	DLT use cases
Technical Specification	FG DLT D3.1	DLT reference architecture
Technical Specification	FG DLT D3.3	Assessment criteria for DLT platforms
Technical Report	FG DLT D4.1	DLT regulatory framework
Technical Report	FG DLT D5.1	Outlook on DLTs

The FG DLT Deliverables are available on the ITU webpage, at https://itu.int/en/ITU-T/focusgroups/dlt/.

For more information about FG DLT and its deliverables, please contact Martin Adolph (ITU) at tsbfgdlt@itu.int.

Technical Specification FG DLT D1.1

Distributed ledger technology terms and definitions

Summary

This technical specification is a deliverable of the ITU-T Focus Group on Application of Distributed Ledger Technology (FG DLT).

It contains a baseline set of definitions of terms commonly used in the context of distributed ledger technology (DLT). The definitions provide a basic characterization of the term, and where appropriate, a note is included to provide additional clarity. The concept and rationale for some of the key terms and definitions is described in Annex A.

Keywords

DLT; distributed ledger technology; ledger; blockchain; terms; definitions

Editors:	Heung Youl Youm Soonchunhyang Univ. Korea (Republic of)	Tel: E-mail:	+82-41-530-1328 hyyoum@sch.ac.kr
	Mee Yeon Kim Soonchunhyang Univ. Korea (Republic of)	Tel: E-mail:	+82-41-530-1328 17kmy@sch.ac.kr
	Skylar Hurwitz Jelurida / Demetrius Consulting Switzerland / United States	Tel: E-mail:	+1 215 792 4226 skylar@jelurida.com

CONTENTS

Page

Technical Specification FG DLT D1.1

Distributed ledger technology terms and definitions

1 Scope

This document contains a baseline set of definitions of terms commonly used in distributed ledger technology (DLT). The definitions provide a basic characterization of the term, and where appropriate, a note is included to provide additional clarity. The concept and rationale for some of the key terms and definitions is described in Annex A.

2 References

None.

3 Definitions

This clause is intentionally left blank.

4 Abbreviations and acronyms

This document uses the following abbreviations:

BaaS	Blockchain as a Service
DAO	Decentralized Autonomous Organization
DLT	Distributed Ledger Technology
PII	Personally Identifiable information

5 Conventions

This clause is intentionally left blank.

6 Terms and definitions

6.1 account: representation of an entity whose data is recorded on a distributed ledger.

6.2 address: identifier for entity(ies) performing transactions or other actions in a blockchain or distributed ledger network.

6.3 application [b-Y.2091]: a structured set of capabilities, which provide value-added functionality supported by one or more services.

6.4 asset: representation of value.

6.5 bitcoin: an example of a blockchain using Proof of Work.

6.6 block: individual data unit of a blockchain, composed of a collection of transactions and a block header.

NOTE – A block may be immutable and considered as the digital entity described in clause 3.2.2 in [b-X.1255], however, it can be applied to other networks or other computational facilities.

6.7 block header [b-ISO/TC 307]: data structure that includes a cryptographic link to the previous block.

6.8 blockchain: 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.

6.9 blockchain as a service (BaaS): a cloud service category in which the capabilities provided to the cloud service customer are to deploy and manage a blockchain network enabling the ability of consensus, smart contract, transaction, crypto engine, block record storage, peer-to-peer connectivity and management using blockchain.

6.10 Byzantine fault tolerance: property that enables a system to continue operating properly even if some of its components fail or existence of intentional bad actors.

6.11 compliance: adherence to specified requirements.

6.12 consensus: agreement that a set of transactions is valid.

6.13 consensus mechanism: rules and procedures by which consensus is reached.

6.14 crash fault tolerance: property that enables a system to continue operating properly even if some of its components fail.

6.15 decentralized application: application that runs in a distributed and decentralized computing environment.

6.16 decentralized autonomous organization (DAO): a digital entity that manages assets and operates autonomously in a decentralized system, but also relies on individuals tasked to perform certain functions that the automaton itself cannot.

6.17 decentralized system [b-ISO/TC 307]: distributed system wherein control is distributed among the persons or organizations participating in the operation of system.

6.18 delegated proof of stake (DPoS): another approach to Proof of Stake where a set number of nodes are elected or selected to function as the block-producing full validating nodes for the network.

6.19 digital signature [b-X.800|ISO 7498-2]: data appended to, or a cryptographic transformation (see cryptography) of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g., by the recipient.

NOTE – Consider the definition 'digital signature' as "Data appended to data units, or cryptographic changes made to data units, which allows the recipient of the data unit to confirm the origin and integrity of the data and protect the data from being forged."

6.20 distributed ledger: a type of ledger that is shared, replicated, and synchronized in a distributed and decentralized manner.

6.21 DLT oracle: service that supplies information to a distributed ledger using data from outside of a distributed ledger system.

6.22 fork: creation of two or more different versions of a distributed ledger.

NOTE – There are two types of forks. See clause 6.25 (hard fork) and clause 6.52 (soft fork).

6.23 genesis block: The first block in a blockchain that serves to initialize the blockchain.

6.24 governance [b-ISO/IEC 38500]: system of directing and controlling.

6.25 hard fork: change to the protocol or rules that result in a fork that is not backward compatible.

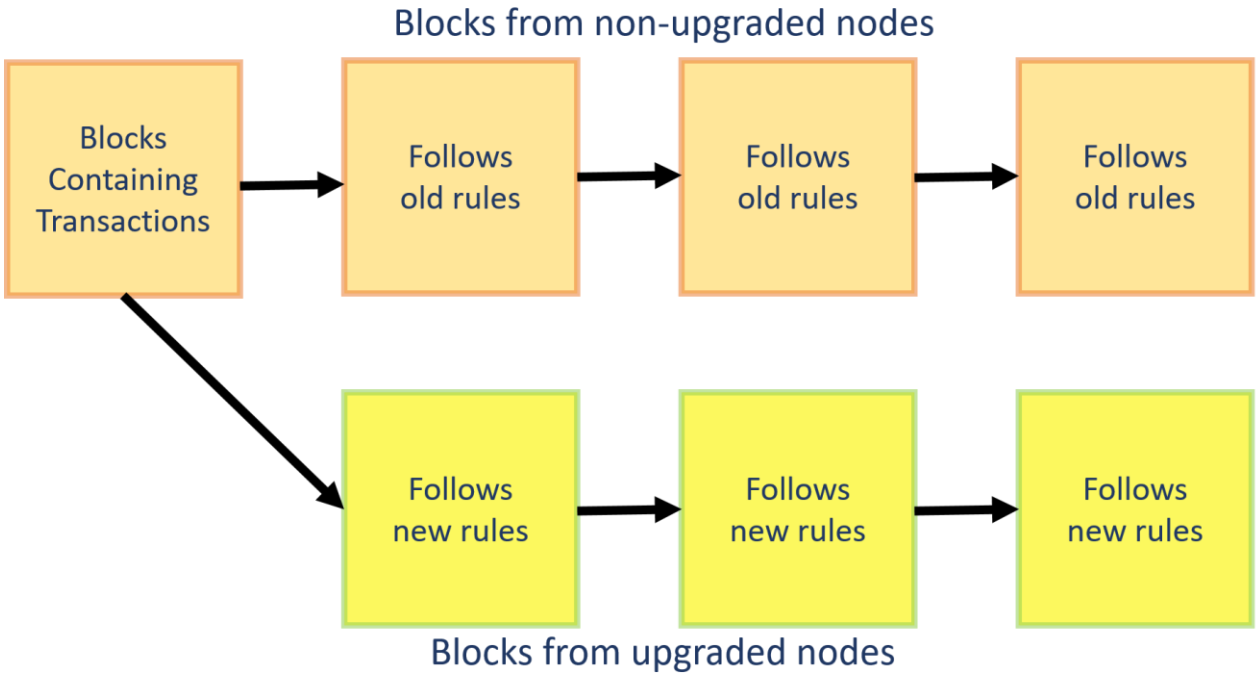

Figure 1 - Hard fork (redrawn from [b-BA])

6.26 hash function [b-NIST]: a function that maps a bit string of arbitrary length to a fixed-length bit string. Approved hash functions satisfy the following properties:

1. One-way: It is computationally infeasible to find any input that maps to any pre-specified output, and

2. Collision resistant: It is computationally infeasible to find any two distinct inputs that map to the same output.

6.27 hashing [b-NIST]: a method of calculating a relatively unique output (called a *hash digest*) for an input of nearly any size (a file, text, image, etc.). The smallest change of input, even a single bit, will result in a completely different output digest.

6.28 hybrid permission: a combination of permissionless and permissioned accessibility.

6.29 immutable [b-ISO/TC 307]: property of blockchain and distributed ledger systems that ledger records can only be added, but not removed or modified, and are designed not to allow changes to historical data over time.

6.30 incentive mechanism [b-ISO/TC 307]: method of offering reward for some activities concerned with the operation of a distributed ledger system.

NOTE – Incentives may be used to encourage the participation of players and/or rewarding for their contributions. Incentives may not be mandatory.

6.31 inter ledger interoperability: ability of two or more distributed ledger protocols to exchange information and to use information that has been exchanged with one another.

6.32 intra ledger interoperability: ability of two or more tokens within distributed ledger platform to operate with one another.

6.33 ledger: information store that keeps final and definitive (immutable) records of transactions.

6.34 Merkle tree [b-NIST]: a data structure where the data is hashed and combined until there is a singular root hash that represents the entire data structure.

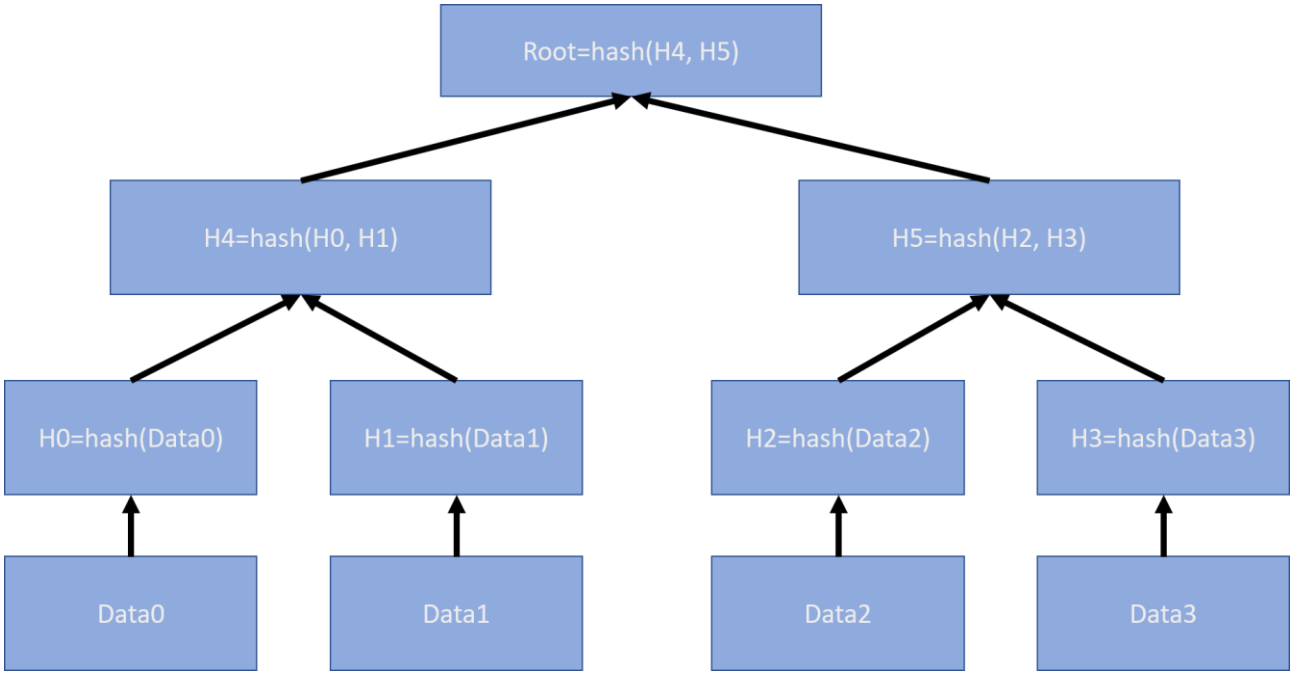

Figure 2 - Example of a Merkle tree (redrawn from [b-NIST])

6.35 node: device or process that participates in a distributed ledger network.

NOTE – Nodes can store a complete or partial replica of the distributed ledger.

6.36 nonfungible token (NFT): an entirely unique digital representation of asset.

6.37 offchain [b-ISO/TC 307]: related to a blockchain system, but located, performed or run outside that blockchain system.

6.38 onchain [b-ISO/TC 307]: located, performed or run inside a blockchain system.

6.39 participant: An actor who can access the ledger: read records or add records to.

6.40 peer-to-peer [b-ISO/TC 307]: relating to, using, or being a network of peers that directly share information and resources with each other without relying on a central entity.

NOTE – In the context of a distributed ledger system, peers are nodes.

6.41 permission [b-NIST]: intended allowable user actions (e.g., participate, read, write, execute).

6.42 permissioned [b-ISO/TC 307]: requiring authorization to perform a particular activity or activities.

6.43 permissionless [b-ISO/TC 307]: not requiring authorization to perform any particular activity.

6.44 permissioned distributed ledger system: distributed ledger system in which permissions are required to maintain and operate a node.

6.45 permissionless distributed ledger system: distributed ledger system where permissions are not required to maintain and operate a node.

NOTE – Examples of permissionless ledger are the Bitcoin and Ethereum blockchains, where any user can join the network and start mining.

6.46 proof of work: consensus process to solve a difficult (costly, time-consuming) problem that produces a result that is easy for others to correctly verify.

NOTE – Producing a proof of work can be a random process with low probability so that a lot of trial and error is required on average before a valid proof of work is generated. Bitcoin uses the Hash cash proof of work system.

6.47 proof of stake: consensus process, where an existing stake in the distributed ledger system (e.g., the amount of that currency that you hold) is used to reach consensus.

6.48 public key cryptography [b-ISO/IEC 2382]: cryptography in which a public key and a corresponding private key are used for encryption and decryption, where public key is disseminated, and private key is known only to the key owner.

NOTE – Users can digitally sign data with their private key, and the resulting signature can be verified by anyone using the corresponding public key.

6.49 public distributed ledger system [b-ISO/TC 307]: distributed ledger system which is accessible to the public for use.

6.50 private distributed ledger system [b-ISO/TC 307]: distributed ledger system which is accessible for use only to a limited group of DLT users.

6.51 smart contract: program written on the distributed ledger system which encodes the rules for specific types of distributed ledger system transactions in a way that can be validated, and triggered by specific conditions.

6.52 soft fork: change to the protocol or rules that result in a fork that is backward compatible.

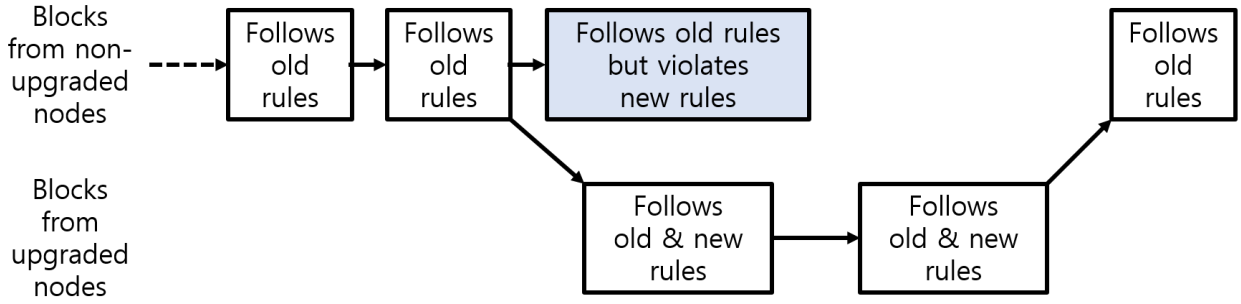

Figure 3 - Soft fork (redrawn from [b-BA])

6.53 subchain [b-ISO/TC 307]: logically separate chain that can form part of a blockchain system.

6.54 stateful contract: contract with specified states.

6.55 stateless contract: contract lacking specified states.

6.56 stateful execution of contract: execution of a program that occurs on all nodes that changes a set of bits representing value information stored on-chain within the contract itself. All nodes that

contain the contract must execute the program in order to change a set of bits representing value information.

6.57 stateless execution of contract: execution of a program that occurs on an individual node (or subset of nodes) that changes a set of bits representing value information stored on-chain but apart from the contract.

6.58 token: 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.

6.59 token ecosystem: digital system or digital space where participants and users interact and coordinate with each other using tokens.

6.60 tokenomics (token economic): economics of a DLT based token.

6.61 transaction: whole of the exchange of information between nodes. A transaction is uniquely identified by a transaction identifier.

6.62 wallet: software and/or hardware used to generate, manage and store both private and public keys and addresses, which enable DLT users to transact. Some wallets may interact with smart contracts and allow single and/or multi-signature.

Annex A: Key points and rationale for DLT basic terminology

A.1 Defining distributed ledger technology

Distributed ledger technologies (DLTs), the most prominent implementation of which is Blockchain, enables large groups of nodes in the distributed ledger networks to reach agreement and record information without the need for a central authority.

A.2 How does DLT operate?

A distributed ledger is a type of ledger that is shared, replicated, and synchronized in a distributed manner. While there are currently several different types of distributed ledgers in existence, they share certain functional characteristics: a capability of ledger network's nodes to communicate directly with each other; a mechanism for nodes on the network to propose the addition of transactions to the block and for computer programs to manage processes; and a consensus mechanism by which the distributed ledger network can validate what is the agreed-upon newly added block.

Specific feature of Blockchain-based solutions distinguishing them from other DLT solutions is the storage of data in groups known as blocks, and that each validated block is cryptographically linked to the previous block, forming an ever-growing chain of data. Instead of being stored in a central location, the ledger is distributed across the nodes which keep their own copy of it. The nodes in the network strive to agree on the same chain of blocks as new valid blocks are being added.

A.3 DLT actors and components

The components involved in the DLT include user, DLT node, DLT service provider, and user groups. These components may belong to a single organization or separate organizations. Figure A.1 illustrates a typical example of components of the distributed ledger technology.

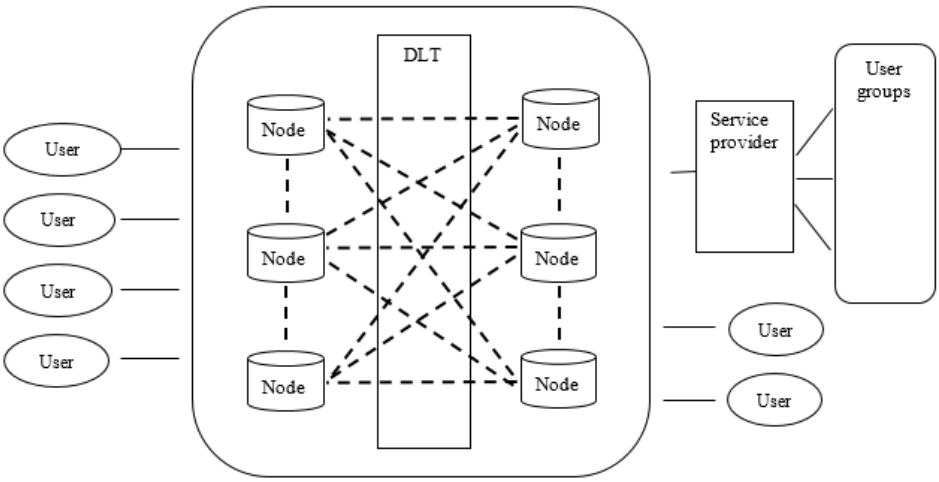

Figure A.1 - A typical example of DLT actors and components

A node is an individual system within the distributed ledger. Some of the nodes known as "full nodes" store the ledger data, pass along the data to other nodes, and ensure that newly added blocks are valid. A service provider is a component that offers a DLT based service to other parties by means of the service interfaces it provides. A user is a component that uses a service or consumes the output of the service provided by another component. A component may be a provider of some services and a consumer of others.

A user group (e.g., groups of people and organizations) is a set of DLT system users. A distributed ledger is information in digital form that has been validated by consensus, replicated, and stored in different nodes.

A.4 Types of DLT

Permissionless distributed ledger systems are decentralized ledger platforms open to anyone validating blocks, without needing permission from any authority. Permissioned distributed ledger systems are ones where users validating blocks shall be authorized.

A.5 Potential use cases for DLT

Distributed ledger technology can be used to decentralize and automate processes in a large number of sectors. The attributes of a distributed ledger technology allow for large numbers of entities or nodes, whether collaborators or competitors, to come to consensus on information and immutably store it.

The potential use cases for a distributed ledger technology are vast. People are looking at distributed ledger technology to disrupt most industries, from automotive, banking, education, energy and e-government to healthcare, insurance, law, music, art, real estate and travel. [b-DLT 2.1] contains an extensive study of DLT use cases.

A.6 Consensus mechanisms

Consensus mechanisms ensure convergence towards a single, immutable version of the ledger. They allow actors on the network to agree on the information recorded on the distributed ledgers, taking into consideration the fact that some actors can be untrustworthy or malicious. The most widespread consensus algorithms are proof-of-work, proof-of-stake and proof-of-authority.

In permissionless distributed ledger networks usually there are numerous validating nodes competing at the same time to validate the next block. They usually do this to obtain newly generated cryptocurrency and/or network transaction fees. They are generally comprised of mutually distrusting users that may only know each other by their public addresses.

A.7 Smart contracts

A smart contract is a computer program that is deployed using cryptographically signed transactions on the distributed ledger network (e.g., Ethereum's smart contracts, Hyperledger Fabric's chaincode). The smart contract is executed by nodes within the distributed ledger system. The results of the execution are validated by consensus and recorded on the distributed ledger.

Smart contract automation reduces costs, lowers risks of errors, mitigates risks of fraud and potentially streamlines many business processes.

Bibliography

In developing this list of DLT terms and definitions, reference has been made to a large number of DLT publications, work and glossaries that already exist.

The list is far from exhaustive but includes:

[b-BBG] IBM Developer, *Blockchain basics: Glossary and use cases*, https://developer.ibm.com/tutorials/cl-blockchain-basics-glossary-bluemix-trs/.

[b-BBT] Dinbits, *Bitcoin & blockchain terminology*, https://news.dinbits.com/p/dinbits-terminology.html.

[b-BA] Bisade A. (2018). *Blockchain Soft Fork & Hard Fork Explained.*

[b-BHG] Blockchain Hub, *Glossary*, https://blockchainhub.net/blockchain-glossary/.

[b-BTG] Blockchain, *Bitcoin glossary*, https://support.blockchain.com/hc/en-us/articles/213276463-Bitcoin-terms-glossary.

[b-DFS] Focus Group Technical Report ITU-T FG DFS:2017, *Digital Financial Services (DFS) Glossary.*

[b-DIN 16597] German National Standard DIN SPEC 16597:2018, *Terminology for blockchain.*

[b-DLT 2.1] Focus Group Technical Report ITU-T FG DLT D2.1:2019, *Distributed ledger technology use cases.*

[b-ISO/IEC 38500] ISO/IEC 38500:2015, *Information Technology -- Governance of IT for the Organization.*

[b-ISO/IEC 2382] ISO/IEC 2382:2015, *Information technology – Vocabulary.*

[b-ISO/TC307] ISO/CD 22739, *Blockchain and distributed ledger technologies – Terminology.*

[b-NIST] NISTIR 8202 (Draft):2018/01, *Blockchain Technology Overview.*

[b-X.800|ISO 7498-2] Recommendation ITU-T X.800|ISO 7498-2:1991, *Security architecture for Open Systems Interconnection for CCITT applications.*

[b-X.1255] Recommendation ITU-T X.1255:2009, *Framework for discovery of identity management information.*

[b-X.das-mgt] Draft Recommendation ITU-T X.das-mgt, *Security framework for the data access and sharing management system based on the distributed ledger technology.*

[b-X.sa-dlt] Draft Recommendation ITU-T X.sa-dlt, *Security assurance for Distributed Ledger Technology.*

[b-X.sct-dlt] Draft Recommendation ITU-T X.sct-dlt, *Security capabilities of, and threats to Distributed Ledger Technology.*

[b-X.sradlt] Draft Recommendation ITU-T X.sradlt, *Security framework for distributed ledger technology.*

[b-X.srdrm-dlt] Draft Recommendation ITU-T X.srdrm-dlt, *Security requirements for digital rights management based on distributed ledger technology.*

[b-X.ss-dlt] Draft Recommendation ITU-T X.ss-dlt, *Security Services based on Distributed Ledger Technology.*

[b-X.stov] Draft Recommendation ITU-T X.stov, *Security threats to online voting using distributed ledger technology*.

[b-X.strdlt] Draft Recommendation ITU-T X.strdlt, *Security threats and requirements of digital payment services based on distributed ledger technology*.

[b-X.tfspd-dlt] Draft Recommendation ITU-T X.tfspd-dlt, *Technical framework for secure software programme distribution mechanism based on distributed ledger*.

[b-Y.2091] Recommendation ITU-T Y.2091:2011, *Terms and definitions for next generation networks.*