International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1400

(10/2020)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Secure applications and services (2) – Distributed ledger technology security

# Terms and definitions for distributed ledger technology

Recommendation ITU-T X.1400

International Telecommunication Union

ITU-T X-SERIES RECOMMENDATIONS

**DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY**

| | |
|---|---|
| PUBLIC DATA NETWORKS | X.1–X.199 |
| OPEN SYSTEMS INTERCONNECTION | X.200–X.299 |
| INTERWORKING BETWEEN NETWORKS | X.300–X.399 |
| MESSAGE HANDLING SYSTEMS | X.400–X.499 |
| DIRECTORY | X.500–X.599 |
| OSI NETWORKING AND SYSTEM ASPECTS | X.600–X.699 |
| OSI MANAGEMENT | X.700–X.799 |
| SECURITY | X.800–X.849 |
| OSI APPLICATIONS | X.850–X.899 |
| OPEN DISTRIBUTED PROCESSING | X.900–X.999 |
| INFORMATION AND NETWORK SECURITY | |
| General security aspects | X.1000–X.1029 |
| Network security | X.1030–X.1049 |
| Security management | X.1050–X.1069 |
| Telebiometrics | X.1080–X.1099 |
| SECURE APPLICATIONS AND SERVICES (1) | |
| Multicast security | X.1100–X.1109 |
| Home network security | X.1110–X.1119 |
| Mobile security | X.1120–X.1139 |
| Web security | X.1140–X.1149 |
| Security protocols (1) | X.1150–X.1159 |
| Peer-to-peer security | X.1160–X.1169 |
| Networked ID security | X.1170–X.1179 |
| IPTV security | X.1180–X.1199 |
| CYBERSPACE SECURITY | |
| Cybersecurity | X.1200–X.1229 |
| Countering spam | X.1230–X.1249 |
| Identity management | X.1250–X.1279 |
| SECURE APPLICATIONS AND SERVICES (2) | |
| Emergency communications | X.1300–X.1309 |
| Ubiquitous sensor network security | X.1310–X.1319 |
| Smart grid security | X.1330–X.1339 |
| Certified mail | X.1340–X.1349 |
| Internet of things (IoT) security | X.1360–X.1369 |
| Intelligent transportation system (ITS) security | X.1370–X.1389 |
| **Distributed ledger technology security** | **X.1400–X.1429** |
| Distributed ledger technology security | X.1430–X.1449 |
| Security protocols (2) | X.1450–X.1459 |
| CYBERSECURITY INFORMATION EXCHANGE | |
| Overview of cybersecurity | X.1500–X.1519 |
| Vulnerability/state exchange | X.1520–X.1539 |
| Event/incident/heuristics exchange | X.1540–X.1549 |
| Exchange of policies | X.1550–X.1559 |
| Heuristics and information request | X.1560–X.1569 |
| Identification and discovery | X.1570–X.1579 |
| Assured exchange | X.1580–X.1589 |
| CLOUD COMPUTING SECURITY | |
| Overview of cloud computing security | X.1600–X.1601 |
| Cloud computing security design | X.1602–X.1639 |
| Cloud computing security best practices and guidelines | X.1640–X.1659 |
| Cloud computing security implementation | X.1660–X.1679 |
| Other cloud computing security | X.1680–X.1699 |
| QUANTUM COMMUNICATION | |
| Terminologies | X.1700–X.1701 |
| Quantum random number generator | X.1702–X.1709 |
| Framework of QKDN security | X.1710–X.1711 |
| Security design for QKDN | X.1712–X.1719 |
| Security techniques for QKDN | X.1720–X.1729 |
| DATA SECURITY | |
| Big Data Security | X.1750–X.1759 |
| 5G SECURITY | X.1800–X.1819 |

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

# Recommendation ITU-T X.1400

## Terms and definitions for distributed ledger technology


### Summary

Recommendation ITU-T X.1400 contains a baseline set of terms and definitions for distributed ledger technology (DLT). The definitions provide a basic characterization of the term, and where appropriate, a note is included to provide additional clarity.

It is based on Focus Group Technical Report ITU-T FG DLT D1.1:2019, *FG DLT D1.1 Distributed ledger technology terms and definitions.*



### History

| Edition | Recommendation | Approval | Study Group | Unique ID* |
|---|---|---|---|---|
| 1.0 | ITU-T X.1400 | 2020-10-29 | 17 | 11.1002/1000/14449 |

### Keywords

Distributed ledger technology, terms and definitions.


* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

## 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, 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/.

## Table of Contents

# Recommendation ITU-T X.1400

## Terms and definitions for distributed ledger technology

### 1 Scope

This Recommendation contains a baseline set of terms and definitions for distributed ledger technology (DLT). The definition of each term provides a basic characterization of the term, and where appropriate, a note is included to provide additional clarity.

### 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.

None.

### 3 Definitions

This clause is intentionally left blank as terms and definitions are presented in clause 6.

### 4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

BaaS Blockchain as a Service

DAO Decentralized Autonomous Organization

DLT Distributed Ledger Technology

DPoS Delegated Proof of Stake

NFT Nonfungible Token

### 5 Conventions

None.

### 6 Terms and definitions related to distributed ledger technology

This Recommendation lists and defines terms related to distributed ledger technology (DLT). The rationale for defining some of the key terms and definitions is presented in Appendix I.

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

**6.2 address**: Identifier for entity(s) performing transactions or other actions in a blockchain or distributed ledger network.

**6.3 application** [b-ITU-T 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 (see clause 6.49).

**6.6 block**: Individual data unit of a blockchain (see clause 6.8), composed of a collection of transactions (see clause 6.65) and a block header.

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

**6.7 block header** [b-ISO/TC 307]: Structured data that includes a cryptographic link to the previous block unless there is no previous block.

NOTE – A block header can also contain a timestamp, a nonce, and other distributed ledger technology (DLT) platform specific data, including a hash value of corresponding transaction records.

**6.8 blockchain**: A type of distributed ledger (see clause 6.21) 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 system** [b-ISO/TC 307]: A system that implements a blockchain.

**6.10 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 in order to enable the abilities of consensus, smart contract, transaction, crypto engine, block record storage, peer-to-peer connectivity and management using blockchain.

**6.11 Byzantine fault tolerance**: Property that enables a system to continue operate properly even if some of its components fail or if there are intentional bad actors.

**6.12 compliance**: Adherence to specified requirements.

**6.13 consensus**: Agreement that a set of transactions is valid.

**6.14 consensus mechanism**: Rules and procedures by which consensus is reached.

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

**6.16 decentralized application**: Application that runs in a distributed and decentralized computing environment.

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

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

**6.19 delegated proof of stake (DPoS)**: Another approach to proof of stake (see 6.50) where a number of nodes are elected or selected to function as the block-producing full validating nodes for the network.

**6.20 digital signature** [b-ITU-T X.800]: 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.

**6.21 distributed ledger**: A type of ledger (see clause 6.36) that is shared, replicated, and synchronized in a distributed and decentralized manner.

**6.22 distributed ledger technology (DLT)** [b-ISO/TC 307]: Technology that enables the operation and use of distributed ledgers.

**6.23 DLT system** [b-ISO/TC 307]: A system that implements a distributed ledger.

**6.24 DLT oracle**: A service that supplies information to a distributed ledger using data from outside of the distributed ledger system.

**6.25 fork**: Creation of two or more different versions of a distributed ledger.

NOTE – There are two types of forks: hard fork (see clause 6.28 and Figure 1) and soft fork (see clause 6.56 and Figure 3).

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

**6.27 governance** [b-ITU-T Y.3514]: System of directing and controlling.

**6.28 hard fork**: Change to the protocol or rules that result in a fork that is not backward compatible.

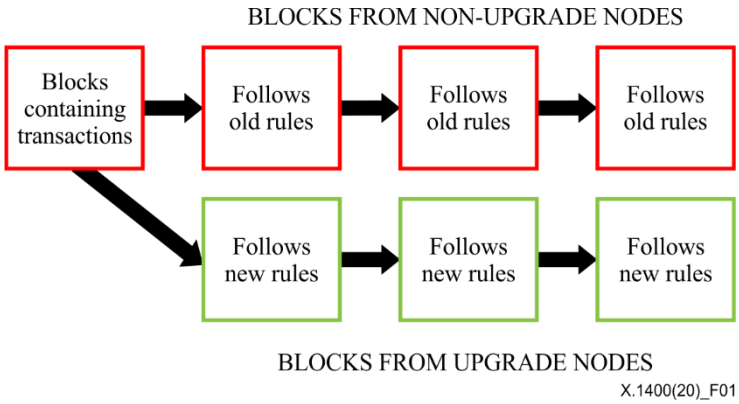


**Figure 1 – Hard fork**

**6.29 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

**6.30 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.

**6.31 hybrid permission**: A combination of permissionless and permissioned accessibility to a distributed ledger system.

**6.32 immutability** [b-ISO/TC 307]: Property of a distributed ledger wherein ledger records cannot be modified or removed once added to a distributed ledger.

NOTE – Where appropriate, immutability also presumes keeping intact the order of ledger records and the links between the ledger records.

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

NOTE – An example of a reward is a block reward.

**6.34 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.

**6.35 intra ledger interoperability**: Ability of two or more tokens within distributed ledger platform to operate with one another.

**6.36 ledger**: Information store that keeps final and definitive (immutable) records of transactions.

**6.37 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.

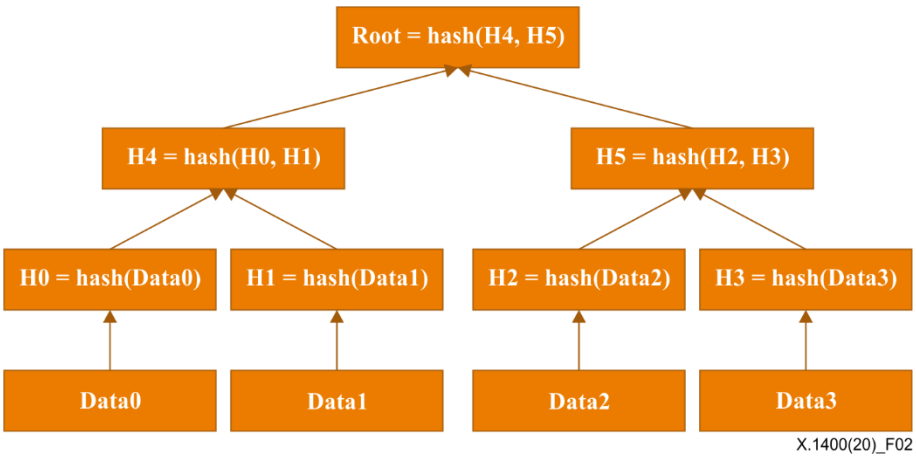


**Figure 2 – Example of a Merkle tree**

**6.38** **node**: Device or process that participates in a distributed ledger network.

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

**6.39** **nonfungible token (NFT)**: An entirely unique digital representation of an asset.

**6.40** **off-chain** [b-ISO/TC 307]: Related to a blockchain system, but located, performed or run outside that blockchain system.

**6.41** **on-chain** [b-ISO/TC 307]: Located, performed or run inside a blockchain system.

**6.42** **participant**: An actor that can access the ledger, read records or add records.

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

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

**6.45** **permissioned** [b-ISO/TC 307]: Requiring authorization to perform a particular activity or activities.

**6.46** **permissionless** [b-ISO/TC 307]: Not requiring authorization to perform any particular activity.

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

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

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

**6.49** **proof of work**: Consensus process to solve a difficult (costly, time-consuming) problem that produces a result that is easy for others to 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.

**6.50** **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.

**6.51** **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 the public key is disseminated, and the 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.

**6.52 public DLT system** [b-ISO/TC 307]: A distributed ledger technology (DLT) system which is accessible to the public for use.

**6.53 private DLT system** [b-ISO/TC 307]: A distributed ledger technology (DLT) system which is accessible for use only to a limited group of DLT users.

**6.54 sidechain** [b-ISO/TC 307]: A blockchain system that interoperates with a separate associated blockchain system to perform a specific function in relation to the associated blockchain system.

NOTE – By convention, the original chain is normally referred to as the "main chain", while any additional blockchains which allow DLT users to transact on the main chain are referred to as "sidechains".

**6.55 smart contract**: A program written on a 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.

**6.56 soft fork**: Change to the protocol or rules that result in a fork that is backward compatible.

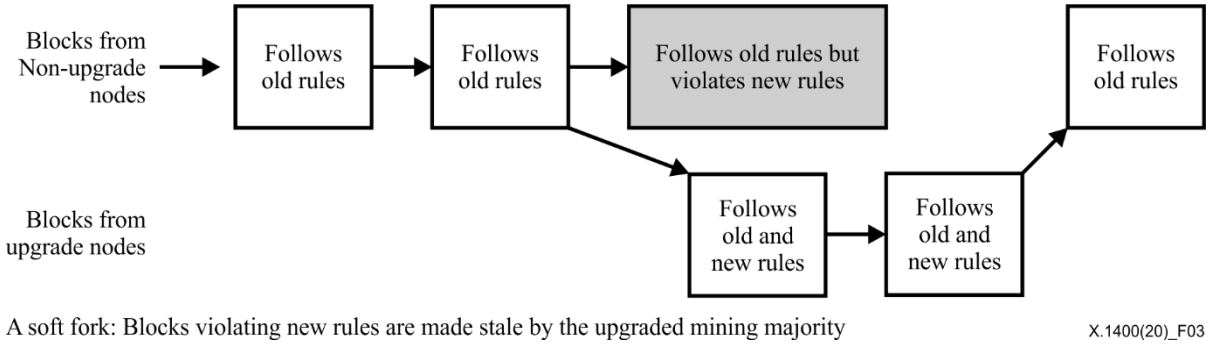


**Figure 3 – Soft fork (adapted from [b-BA])**

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

NOTE – A subchain allows for data isolation and confidentiality.

**6.58 stateful contract**: A contract with specified states.

**6.59 stateless contract**: A contract lacking specified states.

**6.60 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.

**6.61 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.

**6.62 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.

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

**6.64 tokenomics (token economics)**: Economics of a distributed ledger technology (DLT) based token.

**6.65 transaction**: Whole of the exchange of information between nodes. A transaction is uniquely identified by a transaction identifier.

**6.66 wallet**: Software and/or hardware used to generate, manage and store both private and public keys and addresses, which enable distributed ledger technology (DLT) users to transact. Some wallets may interact with smart contracts and allow single and/or multi-signature.

# Appendix I

## Key points and rationale for DLT basic terminology

(This appendix does not form an integral part of this Recommendation.)

### I.1 Defining distributed ledger technology

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

### I.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.

Transaction is a record of exchange status, and addresses are used in transactions to indicate nodes without revealing node itself. Wallet derives addresses from accounts and keep balance of a node's asset, such as cryptocurrencies.

A specific feature of blockchain-based solutions, distinguishing them from other DLT solutions, is the storage of data in groups known as blocks, containing a hash of the previous block, a timestamp and transactions [b-wiki], 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.

Some implementations adopt an incentive mechanism to make nodes engage in publishing a block. The incentive given to a winner which succeed to publish a block is called a block reward.

### I.3 DLT actors and components

The components involved in DLT include users, DLT nodes, DLT service providers 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.

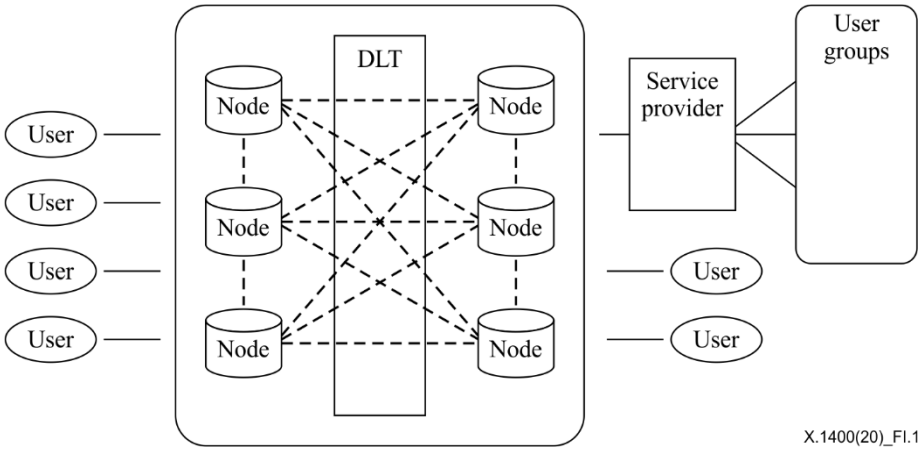


**Figure I.1 – A typical example of DLT actors and components**

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, read/write transactions and blocks, 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.

## I.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 decentralized ledger platforms where users validating blocks must be authorized. The permission can be granted depending on how a system deployed, e.g., authenticated with the accredited certificate, accepted by users, etc.

## I.5 Potential use cases for DLT

A 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 innovate most industries, from automotive, banking, education, energy and e-government to healthcare, insurance, law, music, art, real estate and travel.

## I.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 blockchain, 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.

Distributed ledger is often referred to as decentralized because some of the consensus mechanisms work without a central authority to make decisions. All nodes in the network make decisions individually, and the decisions of each node lead to consensus for its network.

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.

## I.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


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

[b-ITU-T X.1255] Recommendation ITU-T X.1255 (2013), *Framework for discovery of identity management information*.

[b-ITU-T X.1401] Recommendation ITU-T X.1401 (2019), *Security threats to distributed ledger technology*.

[b-ITU-T X.1402] Recommendation ITU-T X.1402 (2020), *Security framework for distributed ledger technology*.

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

[b-ITU-T Y.3514] Recommendation ITU-T Y.3514 (2017), *Cloud computing - Trusted inter-cloud computing framework and requirements*.

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

[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/enus/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-DLT 1.1] Focus Group Technical Report ITU-T FG DLT D1.1:2019, *FG DLT D1.1 Distributed ledger technology terms and definitions*.

[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/TC 307] ISO DIS 22739, *Blockchain and distributed ledger technologies – Terminology*.

[b-NIST] NISTIR 8202:2018/10, *Blockchain Technology Overview*.

[b-wiki] Blockchain at Wikipedia: https://en.wikipedia.org/wiki/Blockchain.

## 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 |

Printed in Switzerland
Geneva, 2021