International Standard

ISO 22739

Second edition
2024-01

Blockchain and distributed ledger technologies — Vocabulary

Chaîne de blocs et technologies de registres distribués — Vocabulaire

Reference number
ISO 22739:2024(en)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 307, *Blockchain and distributed ledger technologies*.

This second edition cancels and replaces the first edition (ISO 22739:2020), which has been technically revised.

The main changes are as follows:

— inclusion of new terms and definitions.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

This document defines terms relating to blockchain and distributed ledger technologies (DLTs) to clarify the meaning of terms and concepts used in other documents within the domain of ISO/TC 307.

Clear, consistent and coherent standards require clear, consistent and coherent terminology. This document follows the rules and guidelines set by ISO/TC 37, *Language and terminology,* for terminology standards.

This document applies to all types of organizations (e.g. commercial enterprises, government agencies and non-profits). The target audience includes but is not limited to academics, solution architects, customers, users, tool developers, regulators, auditors and standards development organizations.

Blockchain and distributed ledger technologies — Vocabulary

1 Scope

This document defines fundamental terminology for blockchain and distributed ledger technologies.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
asset
anything that has value to a stakeholder

[SOURCE: ISO 19299:2020, 3.1, modified — The Note to entry has been removed.]

3.2
block
structured data comprising a *block header* (3.4) and *block data* (3.3)

3.3
block data
structured data comprising zero or more *transaction records* (3.95) or references to transaction records

3.4
block header
structured data that includes a *hash link* (3.47) to the previous *block* (3.2), if present

Note 1 to entry: A block header can also contain a *timestamp* (3.91), a *nonce* (3.62), and other *distributed ledger technology (DLT) platform* (3.33) specific data, including a *hash value* (3.48) of corresponding *transaction records* (3.95).

3.5
block reward
reward given to *miners* (3.59) or *validators* (3.99) after a *block* (3.2) is *confirmed* (3.9) in a *blockchain system* (3.7)

Note 1 to entry: A reward can be in the form of a *cryptoasset* (3.14).

3.6
blockchain
distributed ledger (3.23) with *confirmed blocks* (3.10) organized in an append-only, sequential chain using *hash links* (3.47)

3.7
blockchain system
system that implements a *blockchain* (3.6)

Note 1 to entry: A blockchain system is a type of *distributed ledger technology (DLT) system* (3.35).

3.8
blockchain technology
technology that enables the operation and use of *blockchains* (3.6)

3.9
confirmed
accepted by *consensus* (3.12) to be recorded in a *distributed ledger* (3.23)

3.10
confirmed block
block (3.2) that has been *confirmed* (3.9)

3.11
confirmed transaction
transaction (3.93) that has been *confirmed* (3.9)

3.12
consensus
agreement among *distributed ledger technology (DLT) nodes* (3.31) that:

— a *transaction* (3.93) is *validated* (3.97);

— the *distributed ledger* (3.23) contains a consistent set and ordering of records of validated transactions

Note 1 to entry: Consensus does not necessarily mean that all DLT nodes agree.

Note 2 to entry: The details regarding consensus differ among *DLT systems* (3.35) and this can be a distinguishing characteristic between one DLT system and another.

3.13
consensus mechanism
set of rules and procedures by which *consensus* (3.12) is reached

Note 1 to entry: These rules and procedures are interrelated.

3.14
cryptoasset
crypto-asset
digital asset (3.21) implemented using cryptographic techniques

Note 1 to entry: *distributed ledger technology (DLT) systems* (3.35) can be used to manage or transfer cryptoassets.

3.15
cryptocurrency
cryptoasset (3.14) designed to work as a medium of payment or value exchange

Note 1 to entry: Cryptocurrency involves the use of decentralized control and *cryptography* (3.16) to secure *transactions* (3.93), control the creation of additional *assets* (3.1), and verify the transfer of assets in a *distributed ledger technology (DLT) system* (3.35).

3.16
cryptography
discipline that embodies the principles, means and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modifications

[SOURCE: ISO 7498-2:1989, 3.3.20, modified — The Note to entry has been removed.]

3.17
decentralized application
Dapp
application that runs on a *decentralized system* (3.20)

3.18
decentralized identifier
DID
identifier (3.49) that is issued or managed in a *decentralized system* (3.20) and designed to be unique within a context

Note 1 to entry: Decentralized identifiers are used in systems that do not rely on central registration authorities.

3.19
decentralized identity
identity (3.50) that is managed in a *decentralized system* (3.20)

3.20
decentralized system
distributed system (3.24) wherein control is distributed among the persons or organizations participating in the operation of the system

Note 1 to entry: In a decentralized system, the distribution of control among persons or organizations participating in the system is determined by the system's design.

3.21
digital asset
asset (3.1) that exists only in digital form or that is the digital representation of another asset

3.22
digital signature
data which, when appended to data to be signed, enable the user of the data to authenticate their origin and integrity

[SOURCE: ISO 14641:2018, 3.17, modified — "digital document" has been replaced with "data to be signed".]

3.23
distributed ledger
ledger (3.54) that is shared across a set of *distributed ledger technology (DLT) nodes* (3.31) and synchronized between the DLT nodes using a *consensus mechanism* (3.13)

Note 1 to entry: A distributed ledger is designed to be *immutable* (3.51), tamper-resistant, tamper-evident and append-only, containing final and definitive *ledger records* (3.55) of *confirmed* (3.9) and *validated* (3.97) *transactions* (3.93).

3.24
distributed system
system in which components located on networked computers communicate and coordinate their actions by interacting with each other

3.25
DLT
distributed ledger technology
technology that enables the operation and use of *distributed ledgers* (3.23)

3.26
DLT account
distributed ledger technology account
representation of an *entity* (3.38) participating in a *transaction* (3.93) in a *DLT system* (3.35)

3.27
DLT address
distributed ledger technology address
data element designating the originating source or destination of a *transaction* (3.93)

3.28
DLT bridge
distributed ledger technology bridge
DLT oracle (3.32) that enables *interoperability* (3.52) between a *DLT system* (3.35) and other systems that implement *ledgers* (3.54)

Note 1 to entry: The other systems can also be DLT systems.

3.29
DLT governance
distributed ledger technology governance
system for directing and controlling a *DLT system* (3.35) including the distribution of *on-ledger* (3.68) and *off-ledger* (3.66) decision rights, incentives, responsibilities and accountabilities

3.30
DLT network
distributed ledger technology network
network of *DLT nodes* (3.31) which make up a *DLT system* (3.35)

3.31
DLT node
distributed ledger technology node
device or process that participates in a network and stores a complete or partial replica of the *ledger records* (3.55)

3.32
DLT oracle
distributed ledger technology oracle
service that updates a *distributed ledger* (3.23) using data from outside of a *DLT system* (3.35)

Note 1 to entry: DLT oracles can be used by *smart contracts* (3.88) to access data from sources external to the DLT system.

3.33
DLT platform
distributed ledger technology platform
set of processing, storage and communication *entities* (3.38) that together provide the capabilities of the *DLT system* (3.35) on each *DLT node* (3.31)

3.34
DLT solution
distributed ledger technology solution
solution built using a *DLT system* (3.35) to accomplish some business objectives common to a group of *DLT users* (3.36)

Note 1 to entry: A DLT solution consists of the DLT system with its *DLT nodes* (3.31) and communication networks plus all the *decentralized applications* (3.17) connected to each of the DLT nodes, along with any associated non-DLT systems connected to the DLT system.

3.35
DLT system
distributed ledger system
distributed ledger technology system
system that implements a *distributed ledger* (3.23)

3.36
DLT user
distributed ledger technology user
entity (3.38) that uses services provided by a *DLT system* (3.35)

3.37
double spending
failure (3.39) of a *distributed ledger technology (DLT) platform* (3.33) where the control of a *cryptoasset* (3.14) is incorrectly transferred more than once

Note 1 to entry: Double-spending is most often associated with *cryptocurrency* (3.15).

3.38
entity
person, organization or thing that can be distinguished within a context

Note 1 to entry: An entity can be a person, an organization, a device, a subsystem, a process, or a group of such items.

3.39
failure
loss of ability to perform as required

[SOURCE: IEC 60050-192:2015, 192-03-01, modified — The Notes to entry have been removed.]

3.40
fault tolerance
ability of a functional unit to continue to perform a required function in the presence of faults or errors

[SOURCE: ISO/IEC 2382:2015, 2123055, modified — The admitted term "resilience" has been removed; the Notes to entry have been removed.]

3.41
finality
state of a *ledger record* (3.55) wherein it has become irreversible and cannot be modified or removed

Note 1 to entry: Finality can be probabilistic.

3.42
fungible
capable of mutual substitution among individual units

Note 1 to entry: The individual units can be *digital assets* (3.21), e.g. *tokens* (3.92).

3.43
fungible token
token (3.92) that is *fungible* (3.42)

3.44
genesis block
first *block* (3.2) in a *blockchain* (3.6)

Note 1 to entry: A genesis block has no previous block and serves to initialize the blockchain.

3.45
hard fork
distributed ledger technology (DLT) platform (3.33) in which new *ledger records* (3.55) or *blocks* (3.2) created by the *DLT nodes* (3.31) using the new version of the DLT platform are not accepted as valid by DLT nodes using old versions of the DLT platform

Note 1 to entry: If not adopted by all DLT nodes, a hard fork can result in a *ledger split* (3.56).

3.46
hash function
cryptographic hash function
function that maps strings of bits of variable (but usually upper bounded) length to fixed-length strings of bits, satisfying the following properties:

— for a given output, it is computationally infeasible to find an input which maps to this output;

— for a given input, it is computationally infeasible to find a second input which maps to the same output;

— it is computationally infeasible to find any two distinct inputs that map to the same output

Note 1 to entry: Computational feasibility depends on the specific security requirements and environment. Refer to ISO/IEC 10118-1:2016, Annex C.

[SOURCE: ISO/IEC 10118-1:2016, 3.4, modified — The preferred term "cryptographic hash function" has been added; a third list item has been added.]

3.47
hash link
cryptographic link
reference to data, constructed by applying a *hash function* (3.46) to the data

Note 1 to entry: A cryptographic link is used in the *block header* (3.4) to reference the previous *block* (3.2) in order to create the append-only, sequential chain that forms a *blockchain* (3.6).

Note 2 to entry: A cryptographic link allows for the detection of changes in the data to which it refers.

3.48
hash value
string of bits which is the output of a *hash function* (3.46)

[SOURCE: ISO/IEC 27037:2012, 3.11]

3.49
identifier
representation of an *identity* (3.50)

3.50
identity
set of attributes that distinguishes an *entity* (3.38) in a context

3.51
immutability
property of a *distributed ledger* (3.23) wherein *ledger records* (3.55) cannot be modified or removed once added to that distributed ledger

Note 1 to entry: Where appropriate, immutability also presumes keeping intact the order of ledger records and the links between the ledger records.

Note 2 to entry: Immutability can emerge from the interaction of individual nodes in a *decentralized system* (3.20) even if the ledger records in any given *distributed ledger technology (DLT) node* (3.31) change.

3.52
interoperability
ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged

Note 1 to entry: Interoperability is possible between applications on a single *distributed ledger technology (DLT) system* (3.35), between DLT systems, or between a DLT system and external systems.

[SOURCE: ISO/IEC 17788:2014, 3.1.5, modified — Note 1 to entry has been added.]

3.53
leaf node
node (3.61) that has no child nodes

3.54
ledger
information store that keeps *records* (3.81) of *transactions* (3.93) that are intended to be final, definitive and *immutable* (3.51)

3.55
ledger record
record (3.81) containing *transaction records* (3.95), *hash values* (3.48) of transaction records, or references to transaction records recorded *on-ledger* (3.68)

Note 1 to entry: A reference can be implemented as a *cryptographic link* (3.47).

3.56
ledger split
fork
creation of two or more different versions of a *distributed ledger* (3.23) originating from a common starting point with a single history

3.57
Merkle root
root node (3.83) of a *Merkle tree* (3.58)

3.58
Merkle tree
tree data structure in which every *leaf node* (3.53) is labelled with the *hash value* (3.48) of a data element and every non-leaf node is labelled with the hash value of the labels of its child *nodes* (3.61)

3.59
miner
distributed ledger technology (DLT) node (3.31) that engages in *mining* (3.60)

3.60
mining
activity in some *consensus mechanisms* (3.13) that creates and *validates* (3.98) *blocks* (3.2) or validates *ledger records* (3.55)

Note 1 to entry: Participation in mining is often incentivized by *block rewards* (3.5) and *transaction fees* (3.94).

3.61
node
elementary component from which a data structure is built

3.62
nonce
number or bit string used once in a set of cryptographic operations

Note 1 to entry: A nonce is often random or pseudo-random. It is commonly used to guard against replay attacks, where a message is captured and re-sent by a malicious actor. In some *blockchain systems* (3.7) it is used to modulate *mining* (3.60) during the generation of a new *block* (3.2) and is stored in the *block header* (3.4).

3.63
non-fungible
not capable of mutual substitution among individual units

Note 1 to entry: The individual units can be *digital assets* (3.21), e.g. *tokens* (3.92).

3.64
non-fungible token
NFT
token (3.92) that is *non-fungible* (3.63)

3.65
off-chain
related to a *blockchain system* (3.7) but located, performed or run outside that blockchain system

3.66
off-ledger
related to a *distributed ledger technology (DLT) system* (3.35) but located, performed or run outside that DLT system

3.67
on-chain
located, performed or run inside a *blockchain system* (3.7)

3.68
on-ledger
located, performed or run inside a *distributed ledger technology (DLT) system* (3.35)

3.69
orphan block
previously *confirmed* (3.9) *block* (3.2) that is no longer confirmed

Note 1 to entry: A block can become an orphan block for various reasons, for example, as a result of competition among *miners* (3.59) during the process of achieving *consensus* (3.12).

3.70
peer-to-peer
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* (3.38)

3.71
permissioned
requiring authorization to perform a particular activity or activities

3.72
permissioned DLT system
permissioned distributed ledger system
permissioned distributed ledger technology system
DLT system (3.35) in which permissions are required

3.73
permissionless
not requiring authorization to perform any particular activity

3.74
permissionless DLT system
permissionless distributed ledger system
permissionless distributed ledger technology system
DLT system (3.35) that is *permissionless* (3.73)

3.75
private DLT system
private distributed ledger system
private distributed ledger technology system
DLT system (3.35) that is accessible for use only to a limited group of *DLT users* (3.36)

Note 1 to entry: Public and private categories apply to DLT users, and *permissioned* (3.71) and *permissionless* (3.73) categories apply to DLT users and those *entities* (3.38) that administer or operate the DLT system.

3.76
private key
key of an *entity's* (3.38) asymmetric key pair that is kept secret and that should only be used by that entity

[SOURCE: ISO/IEC 9798-1:2010, 3.22]

3.77
prune
produce a smaller replica of a *distributed ledger* (3.23) by removing all information meeting specified criteria while ensuring that the information can be restored with integrity if needed

3.78
public DLT system
public distributed ledger system
public distributed ledger technology system
DLT system (3.35) that is accessible to the public for use

3.79
public key
key of an *entity's* (3.38) asymmetric key pair that can be made public

[SOURCE: ISO/IEC 9798-1:2010, 3.25]

3.80
public-key cryptography
cryptography (3.16) in which a *public key* (3.79) and a corresponding *private key* (3.76) are used for encryption and decryption, or are used for verifying digital signatures and digitally signing, respectively

3.81
record
information created or received and maintained as evidence and as an *asset* (3.1) by an organization in pursuit of its legal obligations or in the course of conducting business

Note 1 to entry: This term applies to information in any medium, form or format.

[SOURCE: ISO 30300:2020, 3.2.10 — Notes 1 and 2 to entry have been removed and a new Note 1 to entry has been added.]

3.82
reward system
incentive mechanism
method of offering reward for some activities concerned with the operation of a *distributed ledger technology (DLT) system* (3.35)

Note 1 to entry: An example of a reward is a *block reward* (3.5).

3.83
root node
node (3.61) that has no parent node

3.84
security token
token (3.92) with specific characteristics that meets the definition of financial instrument or other investment instrument under applicable legislation in the relevant jurisdiction

3.85
self-sovereign identity
SSI
identity (3.50) that is solely controlled by the *entity* (3.38) that the identity distinguishes

Note 1 to entry: A self-sovereign identity is generally used to protect an entity's autonomy and control over its identities.

Note 2 to entry: Control of an entity's self-sovereign identity can be delegated in some cases.

3.86
shared ledger
distributed ledger (3.23) in which the content of *ledger records* (3.55) is accessible by multiple *entities* (3.38)

3.87
sidechain
blockchain system (3.7) that has *interoperability* (3.52) with a separate associated blockchain system to perform a specific function in relation to the associated blockchain system

Note 1 to entry: By convention the original chain is normally referred to as the "main chain", while any additional *blockchains* (3.6) that allow *distributed ledger technology (DLT) users* (3.36) to transact on the main chain are referred to as "sidechains".

3.88
smart contract
computer program stored in a *distributed ledger technology (DLT) system* (3.35) wherein the outcome of any execution of the program is recorded on the *distributed ledger* (3.23)

Note 1 to entry: A smart contract can represent terms in a contract in law and create a legally enforceable obligation under the legislation of an applicable jurisdiction.

3.89
soft fork
distributed ledger technology (DLT) platform (3.33) that is not a *hard fork* (3.45) and in which some *records* (3.81) or *blocks* (3.2) created by the *DLT nodes* (3.31) using the old version of the DLT platform are not accepted as valid by DLT nodes using new versions of the DLT platform

3.90
subchain
logically separate chain that can form part of a *blockchain system* (3.7)

Note 1 to entry: A subchain allows for data isolation and confidentiality.

3.91
timestamp
time variant parameter that denotes a point in time with respect to a common time reference

[SOURCE: ISO/IEC 18014-1:2008, 3.12, modified — The space between "time" and "stamp" has been removed.]

3.92
token
asset (3.1) that represents a collection of entitlements

3.93
transaction
smallest unit of a work process consisting of one or more sequences of actions required to produce an outcome that complies with governing rules

3.94
transaction fee
fee paid to *miners* (3.59) or *validators* (3.99) for processing a *transaction* (3.93) in a *distributed ledger technology (DLT) system* (3.35)

3.95
transaction record
record (3.81) documenting a *transaction* (3.93) of any type

Note 1 to entry: Transaction records can be included in, or referred to in, a *ledger record* (3.55).

Note 2 to entry: Transaction records can include the result of a *transaction* (3.93).

3.96
utility token
token (3.92) that can be used by its owner to receive access to goods or services

Note 1 to entry: Utility tokens are usually only accepted by the issuer of the token.

3.97
validated
status of an *entity* (3.38) when its required integrity conditions have been checked and met

Note 1 to entry: For example, in a *distributed ledger technology (DLT) system* (3.35), a *transaction* (3.93), *ledger record* (3.55) or *block* (3.2) can be validated.

3.98
validation
function by which a *transaction* (3.93), *ledger record* (3.55) or *block* (3.2) is *validated* (3.97)

3.99
validator
entity (3.38) in a *distributed ledger technology (DLT) system* (3.35) that participates in *validation* (3.98)

Note 1 to entry: In some DLT systems the *DLT node* (3.31) that has the role of validator can digitally sign a *ledger record* (3.55) or *block* (3.2).

3.100
wallet
application or mechanism used to generate, manage, store or use *private keys* (3.76) and *public keys* (3.79) or other *digital assets* (3.21)

Note 1 to entry: A wallet can be implemented in software, implemented as a hardware module, or written onto non-digital media such as paper or metal.

Note 2 to entry: Digital assets stored in wallets can include, for example, *non-fungible tokens* (3.64).