INTERNATIONAL STANDARD

ISO 22739

First edition
2020-07

Blockchain and distributed ledger technologies — Vocabulary

Chaîne de blocs et technologies de registres distribués — Vocabulaire

Reference number
ISO 22739:2020(E)

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 documents 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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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*.

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 basic terms relating to blockchain and distributed ledger technologies to clarify the meaning of terms and concepts used in other document within the domain of ISO/TC 307 standards.

Clear, consistent and coherent standards require clear, consistent and coherent terminology. This document follows 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, not-for-profit organizations). 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 provides 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 terminological databases for use in standardization at the following addresses:

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

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

3.1
asset
anything that has value to a stakeholder

[SOURCE: ISO/TS 19299:2015, 3.3, modified — Note 1 to entry has been removed.]

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

3.3
block data
structured data comprising zero or more *transaction records* (3.79) or references to *transaction records* (3.79)

3.4
block header
structured data that includes a *cryptographic link* (3.16) to the previous *block* (3.2) unless there is no previous *block* (3.2)

Note 1 to entry: A block header can also contain a *timestamp* (3.75), a *nonce* (3.51), and other *DLT platform* (3.29) specific data, including a *hash value* (3.39) of corresponding *transaction records* (3.79).

3.5
block reward
reward given to *miners* (3.48) or *validators* (3.83) after a *block* (3.2) is *confirmed* (3.8) in a *blockchain system* (3.7)

Note 1 to entry: A reward can be in the form of a *token* (3.76) or *cryptocurrency* (3.14).

3.6
blockchain
distributed ledger (3.22) with *confirmed blocks* (3.9) organized in an append-only, sequential chain using *cryptographic links* (3.16)

Note 1 to entry: Blockchains are designed to be tamper resistant and to create final, definitive and *immutable* (3.40) *ledger records* (3.44).

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

Note 1 to entry: A blockchain system is a type of *DLT system* (3.30).

3.8
confirmed
accepted by *consensus* (3.11) for inclusion in a *distributed ledger* (3.22)

3.9
confirmed block
block (3.2) that has been *confirmed* (3.8)

3.10
confirmed transaction
transaction (3.77) that has been *confirmed* (3.8)

3.11
consensus
agreement among *DLT nodes* (3.27) that 1) a *transaction* (3.77) is *validated* (3.81) and 2) that the *distributed ledger* (3.22) contains a consistent set and ordering of *validated* (3.81) *transactions* (3.77)

Note 1 to entry: Consensus does not necessarily mean that all *DLT nodes* (3.27) agree.

Note 2 to entry: The details regarding consensus differ among *DLT* (3.23) designs and this is a distinguishing characteristic between one design and another.

3.12
consensus mechanism
rules and procedures by which *consensus* (3.11) is reached

3.13
crypto-asset
digital asset (3.20) implemented using cryptographic techniques

3.14
cryptocurrency
crypto-asset (3.13) designed to work as a medium of value exchange

Note 1 to entry: Cryptocurrency involves the use of decentralized control and *cryptography* (3.17) to secure *transactions* (3.77), control the creation of additional *assets* (3.1), and verify the transfer of *assets* (3.1).

3.15
cryptographic hash function
function mapping binary strings of arbitrary length to binary strings of fixed length, such that it is computationally costly to find for a given output an input that maps to the output, it is computationally infeasible to find for a given input a second input that maps to the same output, and 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.

3.16
cryptographic link
reference, constructed using a *cryptographic hash function* (3.15) technique, that points to 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).

3.17
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 modification

[SOURCE: ISO 7498-2:1989, 3.3.20, modified — the NOTE has been removed.]

3.18
decentralized application
DApp
application that runs on a *decentralized system* (3.19)

3.19
decentralized system
distributed system (3.32) 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.

3.20
digital asset
asset (3.1) that exists only in digital form or which is the digital representation of another *asset* (3.1)

3.21
digital signature
data which, when appended to a digital object, enable the user of the digital object to authenticate its origin and integrity

[SOURCE: ISO 14641:2018, 3.17, modified —"digital document" has been replaced with "digital object".]

3.22
distributed ledger
ledger (3.43) that is shared across a set of *DLT nodes* (3.27) and synchronized between the DLT nodes using a *consensus mechanism* (3.12)

Note 1 to entry: A distributed ledger is designed to be tamper resistant, append-only and *immutable* (3.40) containing *confirmed* (3.8) and *validated* (3.81) *transactions* (3.77).

3.23
DLT
distributed ledger technology
technology that enables the operation and use of *distributed ledgers* (3.22)

3.24
DLT account
distributed ledger technology account
representation of an *entity* (3.34) participating in a *transaction* (3.77)

Note 1 to entry: A *smart contract* (3.72), *digital asset* (3.20), or one or more *private keys* (3.62), for example, can be associated with a DLT account.

3.25
DLT address
distributed ledger technology address
value that identifies a *DLT account* (3.24) participating in a *transaction* (3.77)

3.26
DLT network
distributed ledger technology network
network of *DLT nodes* (3.27) which make up a *DLT system* (3.30)

3.27
DLT node
distributed ledger technology node
node
<distributed ledger technology> device or process that participates in a network and stores a complete or partial replica of the *ledger records* (3.44)

3.28
DLT oracle
distributed ledger technology oracle
oracle
service that updates a *distributed ledger* (3.22) using data from outside of a *DLT system* (3.30)

Note 1 to entry: DLT oracles are useful for *smart contracts* (3.72) that cannot access sources of data external to the *DLT system* (3.30).

3.29
DLT platform
distributed ledger technology platform
set of processing, storage and communication *entities* (3.34) which together provide the capabilities of the *DLT system* (3.30) on each *DLT node* (3.27)

3.30
DLT system
distributed ledger system
distributed ledger technology system
system that implements a *distributed ledger* (3.22)

3.31
DLT user
distributed ledger technology user
entity (3.34) that uses services provided by a *DLT system* (3.30)

3.32
distributed system
system in which components located on networked computers communicate and coordinate their actions by interacting with each other

3.33
double spending
failure (3.35) of a *DLT platform* (3.29) where the control of a *token* (3.76) or *crypto-asset* (3.13) is incorrectly transferred more than once

Note 1 to entry: Double-spending is most often associated with *cryptocurrency* (3.14).

3.34
entity
item inside or outside an information and communication technology system, such as a person, an organization, a device, a subsystem, or a group of such items that has recognizably distinct existence

3.35
failure
loss of ability to perform as required

[SOURCE: IEC 60050-192:2015, 192-03-01, modified — Notes 1 to 3 to entry have been removed.]

3.36
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; note 1 to 3 to entry have been removed.]

3.37
genesis block
first *block* (3.2) in a *blockchain* (3.6)

Note 1 to entry: A genesis block has no previous *block* (3.2) and serves to initialize the *blockchain* (3.6).

3.38
hard fork
change to a *DLT platform* (3.29) in which new *ledger records* (3.44) or *blocks* (3.2) created by the *DLT nodes* (3.27) using the new version of the *DLT platform* (3.29) are not accepted as valid by *DLT nodes* (3.27) using old versions of the *DLT platform* (3.29)

Note 1 to entry: If not adopted by all *DLT nodes* (3.27), a hard fork can result in a *ledger split* (3.45).

Note 2 to entry: In some contexts, the terms "hard fork" and *"fork"* (3.45) are sometimes used for a *ledger split* (3.45) that results from a hard fork of a *DLT platform* (3.29).

3.39
hash value
string of bits which is the output of a *cryptographic hash function* (3.15)

[SOURCE: ISO/IEC 27037:2012, 3.11, modified — "cryptographic" has been added.]

3.40
immutability
property wherein *ledger records* (3.44) cannot be modified or removed once added to a *distributed ledger* (3.22)

Note 1 to entry: Where appropriate, immutability also presumes keeping intact the order of *ledger records* (3.44) and the links between the *ledger records* (3.44)

3.41
interoperability
ability of two or more systems or applications to exchange information and to mutually use the information that has been exchanged

[SOURCE: ISO/IEC 17788:2014, 3.1.5]

3.42
leaf node
node (3.50) that has no child *nodes* (3.50)

3.43
ledger
information store that keeps *records* (3.67) of *transactions* (3.77) that are intended to be final, definitive and *immutable* (3.40)

3.44
ledger record
record (3.67) containing *transaction records* (3.79), *hash values* (3.39) of *transaction records* (3.79), or references to *transaction records* (3.79) recorded on a *distributed ledger* (3.22)

Note 1 to entry: A reference can be implemented as a *cryptographic link* (3.16).

3.45
ledger split
fork
creation of two or more different versions of a *distributed ledger* (3.22) originating from a common starting point with a single history

3.46
Merkle root
root node (3.69) of a *Merkle tree* (3.47)

3.47
Merkle tree
tree data structure in which every *leaf node* (3.42) is labelled with the *hash value* (3.39) of a data element and every non-leaf node is labelled with the *hash value* (3.39) of the labels of its child *nodes* (3.50)

3.48
miner
DLT node (3.27) which engages in *mining* (3.49)

3.49
mining
activity, in some *consensus mechanisms* (3.12), that creates and *validates* (3.82) *blocks* (3.2) or *validates* (3.82) *ledger records* (3.44)

Note 1 to entry: Participation in mining is often incentivized by *block rewards* (3.5) and *transaction fees* (3.78).

3.50
node
<organization of data> elementary component from which a data structure is built

3.51
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* (3.49) during the generation of a new *block* (3.2) and is stored in the *block header* (3.4)

3.52
off-chain
related to a *blockchain system* (3.7), but located, performed, or run outside that *blockchain system* (3.7)

3.53
off-ledger
related to a *DLT system* (3.30), but located, performed, or run outside that *DLT system* (3.30)

3.54
on-chain
located, performed, or run inside a *blockchain system* (3.7)

3.55
on-ledger
located, performed, or run inside a *DLT system* (3.30)

3.56
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* (3.34)

3.57
permissioned
requiring authorization to perform a particular activity or activities

3.58
permissioned DLT system
permissioned distributed ledger system
permissioned distributed ledger technology system
DLT system (3.30) in which permissions are required

3.59
permissionless
not requiring authorization to perform any particular activity

3.60
permissionless DLT system
permissionless distributed ledger system
permissionless distributed ledger technology system
DLT system (3.30) that is *permissionless* (3.59)

3.61
private DLT system
private distributed ledger system
private distributed ledger technology system
DLT system (3.30) that is accessible for use only to a limited group of *DLT users* (3.31)

Note 1 to entry: Public and private categories apply to *DLT users* (3.31), and *permissioned* (3.57) and *permissionless* (3.59) categories apply to *DLT users* (3.31) and those *entities* (3.34) that administer or operate the *DLT system* (3.30).

3.62
private key
key of an *entity's* (3.34) asymmetric key pair that is kept secret and which should only be used by that *entity* (3.34)

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

3.63
prune
produce a smaller replica of a *distributed ledger* (3.22) by removing all *transaction records* (3.79) meeting specified criteria while ensuring that those *transactions* (3.77) can be restored with integrity if needed

3.64
public DLT system
public distributed ledger system
public distributed ledger technology system
DLT system (3.30) which is accessible to the public for use

3.65
public key
key of an *entity's* (3.34) asymmetric key pair which can be made public

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

3.66
public-key cryptography
cryptography (3.17) in which a *public key* (3.65) and a corresponding *private key* (3.62) are used for encryption and decryption, or are used for verifying digital signatures and digitally signing, respectively

3.67
record
information created, received and maintained as evidence and as an *asset* (3.1) by an organization or person, in pursuit of legal obligations or in the *transaction* (3.77) of business

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

[SOURCE: ISO 15489-1:2016, 3.14, modified — Note 1 to entry has been added.]

3.68
reward system
incentive mechanism
method of offering reward for some activities concerned with the operation of a *DLT system* (3.30)

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

3.69
root node
node (3.50) that has no parent *node* (3.50)

3.70
shared ledger
distributed ledger (3.22) in which the content of *ledger records* (3.44) is accessible by multiple *entities* (3.34)

3.71
sidechain
blockchain system (3.7) that *interoperates* (3.41) with a separate associated *blockchain system* (3.7) to perform a specific function in relation to the associated *blockchain system* (3.7)

Note 1 to entry: By convention the original chain is normally referred to as the "main chain", while any additional *blockchains* (3.6) which allow *DLT users* (3.31) to transact on the main chain are referred to as "sidechains".

3.72
smart contract
computer program stored in a *DLT system* (3.30) wherein the outcome of any execution of the program is recorded on the *distributed ledger* (3.22)

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.

3.73
soft fork
change to a *DLT platform* (3.29) that is not a *hard fork* (3.38) and in which some *records* (3.67) or *blocks* (3.2) created by the *DLT nodes* (3.27) using the old version of the *DLT platform* (3.29) are not accepted as *valid* (3.81) by *DLT nodes* (3.27) using new versions of the *DLT platform* (3.29)

3.74
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.