

FINAL
DRAFT

INTERNATIONAL
STANDARD

ISO/FDIS
22739

ISO/TC 307

Secretariat: SA

Voting begins on:
2020-04-13

Voting terminates on:
2020-06-08

Blockchain and distributed ledger technologies — Vocabulary

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Full standard:
<https://standards.iteh.ai/catalog/standards/sist/eeffc8a8-0fef-4933-8055-5a8e882cc2ad/iso-fdis-22739>

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.



Reference number
ISO/FDIS 22739:2020(E)

© ISO 2020

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
<https://standards.iteh.ai/catalog/standards/sist/eeffc8a8-0fef-4933-8055-5a8e882cc2ad/iso-fdis-22739>



COPYRIGHT PROTECTED DOCUMENT

© ISO 2020

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

	Page
Foreword.....	iv
Introduction.....	v
1 Scope.....	1
2 Normative references.....	1
3 Terms and definitions.....	1
Bibliography.....	10

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
<https://standards.iteh.ai/catalog/standards/sist/eeffc8a8-0fef-4933-8055-5a8e882cc2ad/iso-fdis-22739>

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Full standard:
<https://standards.iteh.ai/catalog/standards/sist/eefbc8a8-0fef-4933-8055-5a8e882cc2ad/iso-fdis-22739>

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Full standard:
<https://standards.iteh.ai/catalog/standards/sist/ee9bc8a8-0fef-4933-8055-5a8e882cc2ad/iso-fdis-22739>

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 a *block header* (3.4) and *block data* (3.3)

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 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 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* (3.27) 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.