ICS 35.240
L70

中华人民共和国国家标准

GB/T XXXXX—XXXX

信息技术 区块链和分布式记账技术 术语

Information Technology—Blockchain and distributed ledger technology —Volcabulary

（ISO 22739:2020,Blockchain and distributed ledger technologies—Vocabulary,IDT）

（征求意见稿）

XXXX - XX - XX 发布　　XXXX - XX - XX 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　次

前　言 II
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
参 考 文 献 12

前　言

本文件按照GB/T 1.1-2020给出的规则起草。

本标准采用翻译法等同采用ISO 22739：2020《区块链和分布式记账技术 术语》。

本标准对ISO 22739：2020做了以下编辑性修改：

——“参考文献”中用国内文件代替ISO 22739：2020的“参考文献”中相对应的国际文件。

——删除ISO和IEC维护用于标准化的技术数据库的地址信息

本标准由全国信息技术标准化技术委员会（SAC/TC 28）提出并归口。

本标准负责起草单位：中国电子技术标准化研究院。

本标准主要起草人：

信息技术 区块链和分布式记账技术 术语

1 范围

本标准界定了区块链和分布式记账技术的基本术语。

2 规范性引用文件

在本文件中，无规范性引用文件。

3 术语和定义

3.1

资产 asset
对利益相关方有价值的任何事物。
注：改写ISO/TS 19299:2015,定义3.3，注已被删除。

3.2

区块 block
由**区块数据**(3.3)和**区块头**(3.4)组成的结构化数据。

3.3

区块数据 block data
由零个或多个**交易记录**（3.79）或对**交易记录**（3.79）的引用组成的结构化数据。

3.4

区块头 block header
包含指向前一个**区块**(3.2)的**密码技术链接**(3.16)（无前一区块除外）的结构化数据。
注：区块头还可以包含**时间戳**(3.75)、**随机数**(3.51)和**分布式记账技术平台**(3.29)其他特定数据，该特定数据包括相应**交易记录**(3.79)的**哈希值**(3.39)。

3.5

区块奖励 block reward
区块链系统(3.7)中，**区块**(3.2)被**确认**(3.8)后给**矿工**(3.48)或**验证者**(3.83)的奖励。
注:奖励可以是**通证**(3.76)或**加密货币**(3.14)的形式。

3.6

区块链 blockchain
使用**密码技术链接**（3.16）将共识确认过的**区块**（3.9）按顺序追加形成的**分布式账本**（3.22）。

注：区块链被设计用来抵抗篡改，并创建最终的、确定的、**不可变(3.40)**的**账本记录(3.44)**。

3.7

区块链系统 blockchain system

实现**区块链（3.6）**的系统。

注：区块链系统是一种**分布式记账技术系统(3.30)**。

3.8

确认的 confirmed

被**共识(3.11)**接受纳入**分布式账本(3.22)**。

3.9

确认的区块 confirmed block

已完成**确认的（3.8）区块（3.2）**。

3.10

确认的交易 confirmed transaction

已完成**确认的（3.8）交易（3.77）**。

3.11

共识 consensus

分布式记账技术节点(3.27)之间的协定:1)**交易(3.77)**是**验证的(3.81)**;2)**分布式账本(3.22)**包含已**验证的(3.81)**且排序一致的**交易(3.77)**集合。

注1：共识并不代表所有分布式记账技术节点(3.27)都同意。

注2：共识的细节在设计不同的分布式记账技术(3.23)之间有所差异，这也是一种设计相较于另一种设计的显著特征。

3.12

共识机制 consensus mechanism

使节点间达成**共识（3.11）**的规则和程序。

3.13

加密资产 crypto-asset

使用加密技术实现的**数字资产（3.20）**。

3.14

加密货币 cryptocurrency

用作价值交换媒介的**加密资产（3.13）**。

注：加密货币涉及使用去中心化控制和**加密(3.17)**来保护**交易(3.77)**、控制额外**资产(3.1)**的创建和验证**资产(3.1)**的转移。

3.15

密码散列函数 cryptographic hash function

将任意长度的二进制串映射为固定长度的二进制串的函数，使得对于已知的输出值，很难计算原始的输入值；对于给定的输入找到另一个输入使得映射到同样的输出是计算不可行的；对于两个相同的输出值，找到任意两个不同的输入是计算不可行的。

注：计算的可行性取决于特定的安全需求和环境。

3.16

密码链接 cryptographic link

使用**密码散列函数(3.15)**技术构造的、指向数据的引用。

注：**区块头(3.4)**中使用密码链接来引用前一个**区块**(3.2)，以创建仅可追加的、有序的链，从而形成**区块链(3.6)**。

3.17

密码学 cryptography

研究数据转换的原则、手段和方法的学科，用于隐藏数据语义内容、防止数据未经授权的使用，或防止数据未被检测的修改。

注：改写ISO 7498-2:1989,定义3.3.20，注已被删除。

3.18

去中心化应用 decentralized application（DApp）

在**去中心化系统(3.19)**上运行的应用程序。

3.19

去中心化系统 decentralized system

分布式系统(3.32)，其控制被分布在参与系统运行的人员或组织之间。

注：在去中心化系统中，参与系统的人员或组织之间的控制分布是由系统设计决定的。

3.20

数字资产 digital asset

仅以数字形式存在的**资产（3.1）**或其他**资产（3.1）**的数字化表示。

3.21

数字签名 digital signature

附加到数字对象的数据，使数字对象的用户能验证其来源和完整性。

注：改写ISO 14641:2018,定义3.17，将“数字文件”改为“数字对象”。

3.22

分布式账本 distributed ledger

在一组**分布式记账技术节点（3.27）**之间共享并使用**共识机制（3.12）**同步的**账本（3.43）**。

注：分布式账本被设计为防篡改、仅可追加和**不可变(3.40)**，包含**确认(3.8)**和**验证的(3.81)交易(3.77)**。

3.23

分布式记账技术 distributed ledger technology（DLT）

能够运行和使用**分布式账本（3.22）**的技术。

3.24

分布式记账技术账户 DLT account

代表参与**交易(3.77)**的**实体(3.34)**。

注：可以与分布式记账技术帐户相关联的，如**智能合约(3.72)**、**数字资产(3.20)**或一个或多个**私钥(3.62)**。

3.25

分布式记账技术地址 DLT address

标识参与**交易(3.77)**的**分布式记账技术帐户(3.24)**的值。

3.26

分布式记账技术网络 DLT network

由构成分布式记账技术系统（3.30）的**分布式记账技术节点（3.27）**组成的网络。

3.27

分布式记账技术节点 DLT node

节点 node

参与网络并存储**账本记录(3.44)**的全部或部分副本的<分布式记账技术>设备或进程。

3.28

分布式记账技术预言机 DLT oracle

预言机 oracle

使用**分布式记账技术系统（3.30）**外部数据更新**分布式账本（3.22）**的服务。

注：分布式记账技术预言机对于不能访问**分布式记账技术系统（3.30）**外部数据源的**智能合约(3.72)**是有用的。

3.29

分布式记账技术平台 DLT platform

处理、存储、通信的**实体（3.34）**的集合，在每个**分布式记账技术节点（3.27）上**提供**分布式记账技术系统（3.30）**的能力。

3.30

分布式记账技术系统 DLT system

分布式账本系统 distributed ledger system

分布式记账技术系统 distributed ledger technology system

实现**分布式账本的系统(3.22)**。

3.31

分布式记账技术用户 DLT user

分布式记账技术用户 distributed ledger technology user

使用**分布式记账技术系统（3.30）**提供的服务的**实体(3.34)**。

3.32

分布式系统 distributed system

位于联网计算机上的组件通过彼此交互进行通信和协调其行为的系统。

3.33

双花 double spending

分布式记账技术平台(3.29)中，通证(3.76)或**加密资产(3.13)**的控制权被错误地转移多次的**故障(3.35)**。

注：双花通常与**加密货币(3.14)**有关。

3.34

实体 entity

在信息和通信技术系统内部或外部的事物，例如人员、组织、设备、子系统或一组可识别的、明确区分的此类事物。

3.35

故障failure

按要求执行能力的丧失。

注：改写IEC 60050-192:2015, 192-03-01,注1-3已被删除。

3.36

容错 fault tolerance

在出现故障或错误的情况下，功能单元继续执行所需功能的能力。

注：改写IEC 60050-192:2015,定义192.03.01，注已被删除。

3.37

创世区块 genesis block

区块链（3.6）中的第一个**区块**（3.2）。

注：创世区块没有前一个**区块(3.2)**，用于初始化**区块链(3.6)**。

3.38

硬分叉 hard fork

分布式记账技术平台(3.29)的改变，其中使用新版本**分布式记账技术平台(3.29)**的**分布式记账技术节点(3.27)**创建的新**账本记录(3.44)**或**区块(3.2)**，不被使用旧版本**分布式记账技术平台(3.29)**的**分布式记账技术节点(3.27)**接受为有效。

注1：如果没有被所有**分布式记账技术节点(3.27)**采用，硬分叉会导致**账本拆分(3.45)**。

注2：在某些上下文中，术语“硬分叉”和**“分叉”(3.45)**有时用于**分布式记账技术平台(3.29)**的硬分叉导致的**账本拆分(3.45)**。

3.39

哈希值 hash value

密码散列函数(3.15)输出的比特串。

注：改写ISO/IEC 27037:2012定义3.11，增加“密码”。

3.40

不变性 immutability

账本记录(3.44)添加到**分布式账本(3.22)**后不能被修改或删除的属性。

注：在适当的情况下，“不变性”还假定保持**账本记录(3.44)**的顺序和**账本记录(3.44)**之间的链接不变。

3.41

互操作性 interoperability

两个或多个系统或应用程序交换信息和相互使用已交换信息的能力。

[ISO/IEC 17788:2014，定义3.1.5]

3.42

叶节点 leaf node

没有子**节点（3.50）**的**节点（3.50）**。

3.43

账本 ledger

保持最终的、确定的和**不可变（3.40）**的**交易（3.77）记录（3.67）**的信息存储。

3.44

账本记录 ledger record

分布式账本(3.22)上的记录(3.67)，包含**交易记录(3.79)、交易记录(3.79)**的**哈希值(3.39)**或**交易记录(3.79)**的引用。

注：引用可以实现为**密码链接(3.16)**。

3.45

账本拆分 ledger split

分叉 fork

从具有单一历史状态的共同起点创建的两个或多个不同版本的**分布式账本(3.22)**。

3.46

默克尔根 Merkle root

默克尔树（3.47）的**根节点（3.69）**。

3.47

默克尔树 Merkle tree

每个**叶节点(3.42)**被标记为其数据元素的**哈希值(3.39)**，每个非叶节点被标记为其子**节点(3.50)标记**的**哈希值(3.39)**的树型数据结构。

3.48

矿工 miner

参与挖矿**（3.49）**的**分布式记账技术节点（3.27）**。

3.49

挖矿 mining

在某些**共识机制**(3.12)中，创建并**验证**(3.82)**区块**(3.2)或**验证**(3.82)**账本记录**(3.44)的活动。

注：参与挖矿的行为通常受到**区块奖励**(3.5)和**交易手续费**(3.78)的激励。

3.50

节点 node

<数据组织>构建数据结构的基本组件。

3.51

一次性数 nonce(number once，解释？)

在一组密码运算中使用一次的数字或比特串。

注：一次性数通常是随机或伪随机的。通常用于防止重放攻击，即消息被恶意捕获并重新发送。在某些**区块链系统**(3.7)中，它用于在新**区块**(3.2)生成期间调整**挖矿**(3.49)行为，并存储在**区块头**(3.4)中。

3.52

链下 off-chain

与**区块链系统**（3.7）相关，位于、执行或运行于**区块链系统**（3.7）之外。

3.53

账本外 off-ledger

与**分布式记账系统**（3.30）相关，位于、执行或运行于**分布式记账系统**（3.30）之外。

3.54

链上 on-chain

位于、执行或运行于**区块链系统**（3.7）中。

3.55

账本内 on-ledger

位于、执行或运行于**分布式记账系统**（3.30）中。

3.56

点对点 peer-to-peer

与对等节点组成的网络相关、使用或作为对等节点组成的网络，这些对等节点相互之间直接共享信息和资源，而不依赖于中心**实体**（3.34）。

3.57

许可的 permissioned

需要获得授权方可执行某个或某些特定活动。

3.58

许可的分布式记账技术系统 permissioned DLT system

许可的分布式记账系统 permissioned distributed ledger system

许可的分布式记账技术系统 permissioned distributed ledger technology system

需要许可的**分布式记账技术系统**（3.30）。

3.59

非许可的 permissionless
不需要获得授权即可执行任何特定活动。

3.60

非许可分布式记账系统 permissionless DLT system
非许可分布式记账系统 permissionless distributed ledger system
非许可分布式技术记账系统 permissionless distributed ledger technology system
非许可的（3.59）分布式记账技术系统（3.30）。

3.61

私有分布式记账技术系统 private DLT system
私有分布式记账系统 private distributed ledger system
私有分布式记账技术系统 private distributed ledger technology system
只允许有限的**分布式记账技术用户(3.31)**组使用的**分布式记账技术系统(3.30)**。
注：公有和私有的分类适用于**分布式记账技术用户(3.31)**，**许可的(3.57)**和**非许可的(3.59)**分类适用于**分布式记账技术用户(3.31)**和管理或运营**分布式记账技术系统(3.30)**的**实体(3.34)**。

3.62

私钥 private key
实体（3.34）的非对称密钥对中的保密密钥，且该保密密钥只由该**实体（3.34）**使用。
[ISO/IEC 9798-1:2010,定义3.22]

3.63

修剪 prune
通过删除所有符合指定规则的**交易记录(3.79)**，生成一个更小的**分布式账本(3.22)**副本，并确保这些**交易(3.77)**在需要时能够被完整地恢复。

3.64

公有分布式记账技术系统 public DLT system
公有分布式记账系统 public distributed ledger system
公有分布式记账技术系统 public distributed ledger technology system
可供公众使用的**分布式记账技术系统（3.30）**。

3.65

公钥 public key
实体（3.34）的非对称密钥对中的可公开密钥。
[ISO/IEC 9798-1:2010,定义3.25]

3.66

公钥密码学 public key cryptography

公钥（3.65）和对应的**私钥**（3.62）分别用于加密和解密，或分别用于验证数字签名和进行数字签名的**密码学**（3.17）。

3.67

记录 record

组织或个人为履行法律义务或在业务**交易**（3.77）中所创建、接收和维护的作为证据和**资产**（3.1）的信息。

注：该术语适用于任何媒介、形式或格式的信息。

[改写ISO 15489-1:2016定义3.14，增加注1]

3.68

奖励制度 reward system

激励机制 incentive mechanism

为与**分布式记账系统**（3.30）运行有关的某些活动提供奖励的方法。

注：奖励的一个例子是**区块奖励**(3.5)。

3.69

根节点 root node

没有父**节点**（3.50）的**节点**(3.50)。

3.70

共享账本 shared ledger

账本记录（3.44）的内容可由多个**实体**（3.34）访问的**分布式账本**（3.22）。

3.71

侧链 sidechain

与另一个相关联的**区块链系统**(3.7)**互操作**(3.41)，以执行与关联的**区块链系统**(3.7)相关的特定功能的**区块链系统**(3.7)。

注：按照惯例，原始链通常被称为“主链”，而任何允许**分布式记账技术用户**(3.31)在主链上进行交易的其他**区块链**(3.6)被称为“侧链”。

3.72

智能合约 smart contract

存储在**分布式记账技术系统**(3.30)中的计算机程序，该程序的任何执行结果都记录在**分布式账本**(3.22)中。

注：智能合约可以在法律上代表合同条款，并在适用司法管辖区的法律下产生可强制执行的义务。

3.73

软分叉 soft fork

分布式记账技术平台(3.29)的一种改变，这种改变不是**硬分叉**(3.38)，该改变中由采用旧版本**分布式记账技术平台**(3.29)的**分布式记账技术节点**(3.27)所创建的某些**记录**(3.67)或**区块**(3.2)不被采用新版本**分布式记账技术平台**(3.29)的**分布式记账技术节点**(3.27)接受为**验证的(3.81)记录**(3.67)或**区块**(3.2)。

3.74

子链 subchain

逻辑上独立的链，可以构成区块链系统（3.7）的一部分。

注：子链支持数据的隔离和保密。

3.75

时间戳 timestamp

时间变量参数，表示以公共时间为参考的时间点。

[改写ISO/IEC 18014-1:2008定义3.12，修改-“时间”和“戳”之间的空格已被删除。]

3.76

代币 token

代表一系列权利的**数字资产(3.20)**。

3.77

交易 transaction

工作流程的最小单元，是产生符合控制规则的结果所需的一个或多个活动序列。

注：在适当的情况下，交易被更狭义地理解为与**区块链(3.6)**或**分布式账本(3.22)**交互相关的工作流程的最小单位。

3.78

交易手续费 transaction fee

为将一笔**交易(3.77)**纳入**分布式账本(3.22)**而支付给**矿工(3.48)**或**验证者(3.83)**的费用。

3.79

交易记录 transaction record

所有类型**交易（3.77）**的历史**记录（3.67）**。

注 1：交易记录可以包括在**账本记录（3.44）**中或被**账本记录（3.44）**引用。

注 2：交易记录可以包括**交易(3.77)**的结果。

3.80

信任 trust

用户或其他利益相关者对产品或系统将按照该用户或其他利益相关者的预期运行的信心程度。

3.81

验证的 validated

当实体所需的完整性条件已被核验时，**实体(3.34)**的状态。

注：例如，在**分布式记账技术系统(3.30)**中，可以核验**交易(3.77)**、**账本记录(3.44)**或**区块(3.2)**。

3.82

验证 validation

使交易(3.77)、**账本记录(3.44)**或**区块(3.2)**是已**验证的(3.81)**机制。

3.83

验证者 validator

分布式记账技术系统(3.30)中参与**验证**（3.82）的**实体**(3.34)。

注：在某些**分布式记账技术系统**(3.30)中，作为验证者的**分布式记账技术节点**(3.27)可以对**账本记录**(3.44)或**区块**(3.2)进行数字签名。

3.84

钱包 wallet

用于生成、管理、存储或使用**私钥**（3.62）和**公钥**（3.65）的应用。

注：钱包可以实现为软件或硬件模块。

参 考 文 献

[1] ISO 22739 区块链和分布式记账技术 术语（Blockchain and distributed ledger technologies -- Vocabulary）

[2] CBD-Forum-001-2017 区块链 参考架构