中国区块链技术和产业发展论坛标准

CBD-Forum-002-2017

区块链 数据格式规范

Blockchain—Data format specification

2017- 12 - 22 发布

目 次

前言 III
1 范围 1
2 术语和缩略语 1
2.1 其他标准中定义的术语 1
2.2 缩略语 2
3 数据对象结构 2
4 数据分类 3
5 数据元属性 3
6 数据格式规范 3
6.1 账户数据格式 3
6.2 区块数据格式 5
6.3 事务数据格式 8
6.4 实体数据格式 9
6.5 合约数据格式 11
6.6 配置数据格式 12
附录 A （资料性附录） 数据项标识符 15
附录 B （资料性附录） 共识机制相关数据格式 16
B.1 类拜占庭容错 16
B.2 基于权益的证明 19
B.3 基于工作量的证明 20
参考文献 21

前　言

本标准按照GB/T 1.1-2009 给出的规则起草。

本标准由中国区块链技术和产业发展论坛提出。

本标准负责起草单位：中国电子技术标准化研究院、中国万向控股有限公司、浙江蚂蚁小微金融服务集团有限公司、深圳前海微众银行股份有限公司、乐视联服信息技术（北京）有限公司、万达网络科技集团有限公司、中国平安保险（集团）股份有限公司、上海金丘实业股份有限公司、上海钜真金融信息服务有限公司、鑫苑（中国）置业有限公司、众安信息技术服务有限公司、上海分布信息科技有限公司、用友网络科技股份有限公司、海航科技集团有限公司、三一集团有限公司。

本标准主要起草人：李鸣，唐晓丹，谭智勇，张开翔，季宙栋，周平，吴小川，赵博然，华正皓，陈家乐，宋文鹏，周子焱，李斌，李俊，左鹏，李奕，李彦博，金龙，杜宇，姚辉亚，韩梅，杨宝刚，李佳秾，罗荣阁，胡丹青，郝玉琨，董长江，高西林，杜君君，朱天阳，倪旻，易锋平，孙琳，周政军，李升林。

使用帮助信息：任何单位和个人在使用本标准的过程中，若存在疑问，或有对本标准的改进建议和意见，请与中国电子技术标准化研究院（中国区块链技术和产业发展论坛 秘书处）联系。

电话：010-64102801/2804；电子邮件：cbdforum@cesi.cn

通信地址：北京市东城区安定门东大街1号（100007）

为了推动本标准的持续改进，使其内容更加贴近用户组织的实际需求，欢迎社会各方力量参加本标准的持续改进，本标准的更多信息欢迎关注中国区块链技术和产业发展论坛官方网站和公众号。

http://www.cbdforum.cn

区块链 数据格式规范

1 范围

本标准规定了区块链的数据格式规范。具体规定了以下内容：

a） 区块链技术相关的数据结构；

b） 区块链技术相关的数据分类及其相互关系；

c） 区块链技术相关的数据元的数据格式要求。

本标准适用于：

a） 为计划使用区块链的组织建设区块链系统提供数据格式参考；

b） 指导区块链服务提供组织建立区块链系统数据结构；

c） 为区块链系统建设过程的中间件服务组织提供数据格式参考。

2 术语和缩略语

2.1 其他标准中定义的术语

GB/T 19488.1-2004、GB/T 18391.2-2009、GB/T 18391.1-2002 和 CBD-Forum-001-2017 界定的以下术语和定义适用于本文件。

2.1.1

属性 attribute

一个对象或实体的特征。

[GB/T 18391.2-2009]

2.1.2

区块链 blockchain

一种在对等网络环境下，通过透明和可信规则，构建不可伪造、不可篡改和可追溯的块链式数据结构，实现和管理事务处理的模式。

注：事务处理包括但不限于可信数据的产生、存取和使用等。

[CBD-Forum-001-2017]

2.1.3

数据元 data element

通过定义、标识、表示和允许值等一系列属性描述的一个数据单元。

[GB/T 19488.1-2004]

2.1.4

数据类型 data type

由数据元操作决定的用于采集字母、数字和（或）符号的格式，以描述数据元的值。

[GB/T 18391.1-2002]

2.1.5

标识符 identifier
数据元的唯一标识。
[GB/T 18391.1-2002]

2.1.6

智能合约 smart contract
以数字形式定义的能够自动执行条款的合约。
注：在区块链技术领域，智能合约是指基于预定事件触发、不可篡改、自动执行的计算机程序。
[CBD-Forum-001-2017]

2.2 缩略语

下列缩略语适用于本标准。

PKI　　公钥基础设施（Public Key Infrastructure）
ID　　标识（Identity）

3 数据对象结构

区块链技术相关的数据对象结构包括上述区块、事务、实体、合约、账户、配置六个主要数据对象。其中区块链核心的数据对象包括区块、事务、实体和合约。每一区块数据对象中包含一个或多个事务数据对象，每个事务对象包括属性类的实体数据对象，还包括事务的业务逻辑，即合约数据对象。在区块链核心数据对象之外，包括配置数据对象，提供区块链系统正常运行过程中所需的配置信息。配置数据对象和区块链核心数据对象共同构建了区块链运行所需的基础数据基础。而账户数据对象表示区块链业务的实际发起者和相关方对应的数据结构。图 1 给出了数据视图相关的实体间关系。

注： 区块链技术数据结构中所包含的关键要素是区块链技术中涉及到的必要数据，在不同区块链技术相关的平台中可能包含其他非必要数据未在本标准的范围中。

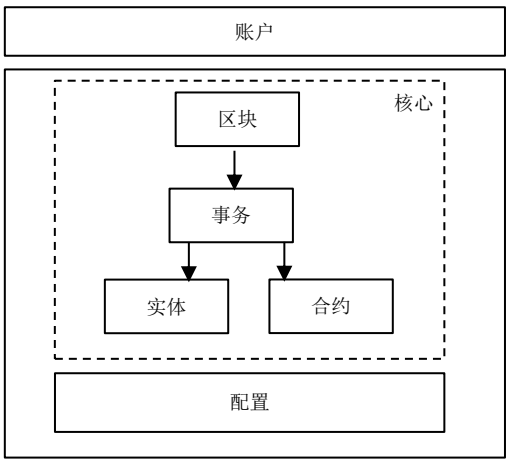

图 1

4 数据分类

本标准以数据对象的类别为依据，将区块链数据分为以下六类：

a）账户数据：指描述区块链事务的实际发起者和相关方的数据。区块中记录的事务信息均被关联到相关的账户之上，每个区块链服务客户拥有一个或多个账户来使用区块链服务。

b）区块数据：指区块链网络的底层链式数据，用来把一段给定时间内发生的事务处理结果持久化为成块链式数据结构。通常情况下，区块由区块头和区块体组成。区块头包含区块相关的控制信息，区块体包含具体的事务数据。

c）事务数据：指描述区块链系统上承载的具体业务动作的数据。其中，事务既包括交易类型事务，也包括非交易类型事务。

d）实体数据：指描述事务的静态属性的数据。通常包括发起方地址、接收方地址、交易发生额、交易费用、存储数据和实体数据备注。

e）合约数据：指描述事务的动态处理逻辑的数据。合约又称智能合约，是一套以计算机代码形式定义的承诺，以及合约参与方可执行承诺的协议。这里的合约数据既包括处理逻辑的可执行代码，也包括处理逻辑的执行结果。

f）配置数据：指区块链系统正常运行过程中所需的配置信息。通常包括共识协议版本号、软件版本号和网络通信底层对等节点配置信息等。

5 数据元属性

区块链数据元通过数据标识符、中文名称、英文名称、数据类型、数据长度、数据说明、数据备注7个属性来描述。具体属性说明见表1。

表1

属性名称	属性说明
数据标识符	各数据元的唯一标识，编号是以阶层式分类，分别将数据分类和数据元依顺序进行流水号编码记录。前段码为数据分类号码，后段码以数据元的流水号，详见附录A。
中文名称	数据元的中文名称，在一定语境下名称应保持唯一。
英文名称	数据元的英文名称，在一定语境下名称应保持唯一。
数据类型	描述数据元的特征和基本要素，本标准中使用的数据类型主要包括：字符串类型、整数类型、数组类型。
数据长度	描述该数据元的长度，在本标准中用定长或不定长表示，并给出了推荐字节长度。
数据说明	详细描述该数据元的内容和表达的含义。
数据备注	描述该数据元是否必要，在本标准中分为必选和可选。

第6章给出了对各种区块链数据元属性的说明和要求。对各数据元的数据标识符的参考性规范见附录A。

6 数据格式规范

6.1 账户数据格式

账户数据主要包括以下几种数据元：

a）账户公钥；

b）账户私钥；

c）账户资产；
d）数字证书；
e）账户所属机构。

6.1.1 账户公钥

账户公钥的数据格式要求见表2。

表2

属性	内容
中文名称	账户公钥
英文名称	Account Public Key
数据类型	字符串
数据长度	定长，推荐64字节
数据说明	根据PKI体系为用户生成的密钥对里，可公开的部分。
数据备注	必选

6.1.2 账户私钥

账户私钥的数据格式要求见表3。

表3

属性	内容
中文名称	账户私钥
英文名称	Account Private Key
数据类型	字符串
数据长度	定长，推荐32字节
数据说明	根据PKI体系为用户生成的密钥对里，不公开的部分。
数据备注	必选

6.1.3 账户资产

账户资产的数据格式要求见表4。

表4

属性	内容
中文名称	账户资产
英文名称	Account Asset
数据类型	数组
数据长度	不定长
数据说明	账户拥有的资产说明，包括资产名称，资产列表，余额等。
数据备注	可选

6.1.4 数字证书

数字证书的数据格式要求见表5。

表5

属性	内容
中文名称	数字证书
英文名称	Digital Certificate
数据类型	数组
数据长度	不定长
数据说明	数字证书是一个经证书授权中心数字签名的包含公开密钥拥有者信息以及公开密钥的文件。
数据备注	可选

6.1.5 账户所属机构

账户所属机构的数据格式要求见表6。

表6

属性	内容
中文名称	账户所属机构
英文名称	Institution
数据类型	数组
数据长度	不定长
数据说明	机构为加入到区块链网络的，独立运作的成员，可以为企业，组织，团体等，账户可以在组织关系上归属于某个机构。
数据备注	可选

6.2 区块数据格式

区块数据主要包括以下几种数据元：

a）区块高度；

b）区块标识；

c）版本信息；

d）前一区块摘要值；

e）默克尔树根；

f）区块时间戳；

g）区块随机数；

h）难度系数；

i）事务列表。

6.2.1 区块高度

区块高度的数据格式要求见表7。

表7

属性	内容
中文名称	区块高度
英文名称	Block Height
数据类型	整数
数据长度	定长
数据说明	标识区块序号，描述区块在区块链中的位置。

属性	内容
数据备注	可选

6.2.2 区块标识

区块标识的数据格式要求见表8。

表8

属性	内容
中文名称	区块标识
英文名称	Block ID
数据类型	字符串
数据长度	定长，推荐长度32字节
数据说明	通常指区块摘要，区块在区块链中的唯一标识。
数据备注	必选

6.2.3 版本信息

版本信息的数据格式要求见表9。

表9

属性	内容
中文名称	版本信息
英文名称	Block Version
数据类型	字符串
数据长度	不定长
数据说明	当前区块版本号，主要对应当前区块头的结构及各个字段的含义。
数据备注	可选

6.2.4 前一区块摘要值

前一区块摘要值的数据格式要求见表10。

表10

属性	内容
中文名称	前一区块摘要值
英文名称	Previous Block Hash
数据类型	字符串
数据长度	定长，推荐长度32字节
数据说明	通常指前一区块的区块摘要，区块在区块链中的唯一标识。
数据备注	必选

6.2.5 默克尔树根

默克尔树根的数据格式要求见表11。

表11

属性	内容
中文名称	默克尔树根

属性	内容
英文名称	Merkle Tree Root
数据类型	字符串
数据长度	定长，推荐长度32字节
数据说明	由本区块里相关的信息通过树状结构算法汇总生成的摘要值。
数据备注	事务树根必选，状态和回执树根可选

6.2.6 区块时间戳

区块时间戳的数据格式要求见表12。

表12

属性	内容
中文名称	区块时间戳
英文名称	Block Timestamp
数据类型	整数
数据长度	定长，推荐长度8字节
数据说明	表示本区块的生成时间刻度（正整数），从1970年起的时间计数，精度为毫秒数，正序增加。
数据备注	必选

6.2.7 区块随机数

区块随机数的数据格式要求见表13。

表13

属性	内容
中文名称	区块随机数
英文名称	Block Nonce
数据类型	整数
数据长度	定长
数据说明	区块随机数，通常用于记账节点竞争记账权的Hash计算的可变参数。
数据备注	可选

6.2.8 难度系数

难度系数的数据格式要求见表14。

表14

属性	内容
中文名称	难度系数
英文名称	Difficulty
数据类型	整数
数据长度	定长，推荐长度8字节
数据说明	通常用于表示记账节点竞争记账权的Hash计算难度的参数。
数据备注	可选

6.2.9 事务列表

事务列表的数据格式要求见表15。

表15

属性	内容
中文名称	事务列表
英文名称	Transaction List
数据类型	数组
数据长度	不定长
数据说明	区块中的事务列表，每个事务通常表示一个业务操作。
数据备注	必选

6.3 事务数据格式

事务数据主要包括以下几种数据元：

a）事务标识；

b）事务类型；

c）签名者；

d）事务时间戳。

6.3.1 事务标识

事务标识的数据格式要求见表16。

表16

属性	内容
中文名称	事务标识
英文名称	Transaction ID
数据类型	字符串
数据长度	定长
数据说明	事务处理中，可保证事务数据的唯一标识，通常为哈希值。
数据备注	必选

6.3.2 事务类型

事务类型的数据格式要求见表17。

表17

属性	内容
中文名称	事务类型
英文名称	Transaction Type
数据类型	字符串或整数
数据长度	定长
数据说明	进行事务操作时，定义事务操作的事件类型，可以有一或多种类型。
数据备注	可选

6.3.3 签名者

签名者的数据格式要求见表18。

表18

属性	内容
中文名称	签名者
英文名称	Signers
数据类型	字符串
数据长度	定长
数据说明	进行事务操作时，对事务进行签名的签名者的集合。
数据备注	可选

6.3.4 事务时间戳

事务时间戳的数据格式要求见表19。

表19

属性	内容
中文名称	事务时间戳
英文名称	Transaction Timestamp
数据类型	整数
数据长度	32字节
数据说明	正整数，从1970年起的时间计数，精度为毫秒，正序增加。
数据备注	可选

6.4 实体数据格式

实体数据主要包括以下几种数据元：

a）发起方地址；

b）接收方地址；

c）事务处理发生额；

d）事务处理费用；

e）附件数据；

f）实体数据备注。

6.4.1 发起方地址

发起方地址的数据格式要求见表20。

表20

属性	内容
中文名称	发起方地址
英文名称	Sender Address
数据类型	字符串
长度	定长
说明	事务操作的发起者或源账户，作为该事务发起方的唯一标识。
备注	必选

6.4.2 接收方地址

接收方地址的数据格式要求见表21。

表21

属性	内容
中文名称	接收方地址
英文名称	Recipient Address
数据类型	字符串
数据长度	定长
数据说明	事务操作中的接收方，作为事务操作对象的唯一标识。
数据备注	可选

6.4.3 事务处理发生额

事务处理发生额的数据格式要求见表22。

表22

属性	内容
中文名称	事务处理发生额
英文名称	Transaction Amount
数据类型	整数或字符串
数据长度	定长
数据说明	事务操作中涉及到账户资产的变更数量，交易额。
数据备注	可选

6.4.4 事务处理费用

事务处理费用的数据格式要求见表23。

表23

属性	内容
中文名称	事务处理费用
英文名称	Transaction Fee
数据类型	整数或字符串
数据长度	定长
数据说明	事务操作中通常会产生一定的交易费用，以防止垃圾交易、流量攻击等。
数据备注	可选

6.4.5 附加数据

附加数据的数据格式要求见表24。

表24

属性	内容
中文名称	附加数据
英文名称	Additional Data
数据类型	字符串
数据长度	定长
数据说明	为部分业务需要提供的备选字段，可增加与业务需求相关的附加数据。
数据备注	可选

6.4.6 实体数据备注

实体数据备注的数据格式要求见表25。

表25

属性	内容
中文名称	实体数据备注
英文名称	Memo
数据类型	字符串
数据长度	不定长
数据说明	事务操作中，可对应该事务的text、ID和hash类型的备注字段。
数据备注	可选

6.5 合约数据格式

合约数据主要包括以下几种数据元：

a）合约标识；

b）合约版本号；

c）合约代码；

d）合约存储。

6.5.1 合约标识

合约标识的数据格式要求见表26。

表26

属性	内容
中文名称	合约标识
英文名称	Contract ID
数据类型	字符串
数据长度	定长
数据说明	合约在区块链上部署后，通过一个唯一的确定的地址标识，供调用方访问合约的代码，状态存储等。
数据备注	该标识一般由创建该合约的账户信息+序列号+其他合约信息（可选）通过可选的摘要算法生成，要求生成的标识唯一，确定，可用。可选

6.5.2 合约版本号

合约版本号的数据格式要求见表27。

表27

属性	内容
中文名称	合约版本号
英文名称	Contract Version
数据类型	字符串
数据长度	不定长
数据说明	针对智能合约的代码和编译发布到区块链上的二进制代码数据，使用版本号标识不同的版本。
数据备注	某个智能合约持续提供某个业务功能，但因需求更迭，或面向不同的问题域而具备不同的特性，需要进行版本划分。可选

6.5.3 合约代码

合约代码的数据格式要求见表28。

表28

属性	内容
中文名称	合约代码
英文名称	Contract Code
数据类型	字符串
数据长度	不定长
数据说明	合约的可执行指令，经过指定编译器编译生成，供区块链上的虚拟机调用执行。
数据备注	根据不同的虚拟机体系，合约代码采用不同的计算机语言编写，并由不同的编译器生成二进制可执行指令。可选

6.5.4 合约存储

合约存储的数据格式要求见表29。

表29

属性	内容
中文名称	合约存储
英文名称	Contract Storage
数据类型	数组
数据长度	不定长
数据说明	合约执行过程生成的状态数据的集合，其内容与合约的逻辑密切相关。
数据备注	可采用key-value格式或关系型数据库保存。可选

6.6 配置数据格式

配置数据主要包括以下几种数据元：

a）协议版本号；

b）版本软件号；

c）节点标识；

d）节点地址；

e）节点公钥。

6.6.1 协议版本号

协议版本号的数据格式要求见表30。

表30

属性	内容
中文名称	协议版本号
英文名称	Protocol Version
数据类型	字符串
数据长度	不定长
数据说明	针对区块链节点之间以及外部应用和区块链节点通信，交互的协议，使用版本号标识不同的协议版本。
数据备注	区块链协议可以随着软件版本升级，具备不同的接口，功能，一般区块链软件应在协议层面向下兼容，

属性	内容
	采用协议版本号进行区分，一套软件可以对使用不同的协议的各种客户端提供服务。可选

6.6.2 软件版本号

软件版本号的数据格式要求见表31。

表31

属性	内容
中文名称	软件版本号
英文名称	Software Version
数据类型	字符串
数据长度	不定长
数据说明	针对区块链软件本身,含代码和二进制软件形态，使用版本号标识不同的发行版本。
数据备注	区块链软件可以针对不同的软件生命周期，以及不同的应用场景，不同的目标用户，采用不同的版本。必选

6.6.3 节点标识

节点标识的数据格式要求见表32。

表32

属性	内容
中文名称	节点标识
英文名称	Peer ID
数据类型	字符串
数据长度	不定长
数据说明	区块链节点的唯一标识，可选用节点的公钥做为唯一标识。
数据备注	必选

6.6.4 节点地址

节点地址的数据格式要求见表33。

表33

属性	内容
中文名称	节点地址
英文名称	Peer Address
数据类型	字符串
数据长度	按照IPv4和IPv6定义长度不定
数据说明	区块链网络节点的IP地址。
数据备注	必选

6.6.5 节点公钥

节点公钥的数据格式要求见表34。

表34

属性	内容
中文名称	节点公钥
英文名称	Peer Public Key
数据类型	字符串
数据长度	定长
数据说明	区块链网络节点的公钥信息。
数据备注	可选

附 录 A
（资料性附录）
数据项标识符

区块链数据元参考标识见表A.1。

表A.1

数据分类	数据元	数据标识
账户数据	账户公钥	01_001
	账户私钥	01_002
	账户资产	01_003
	数字证书	01_004
	账户所属机构	01_005
区块数据	区块高度	02_001
	区块标识	02_002
	版本信息	02_003
	前一区块摘要值	02_004
	默克尔树根	02_005
	区块时间戳	02_006
	难度系数	02_007
	随机数	02_008
	事务列表	02_009
事务数据	事务标识	03_001
	事务类型	03_002
	签名者	03_003
	事务时间戳	03_004
实体数据	发起方地址	04_001
	接收方地址	04_002
	交易发生额	04_003
	交易费用	04_004
	附加数据	04_005
	实体数据备注	04_006
合约数据	合约标识	05_001
	合约版本号	05_002
	合约代码	05_003
	合约存储	05_004
配置数据	共识协议版本号	06_001
	软件版本号	06_002
	节点标识	06_003
	节点地址	06_004
	节点公钥	06_005

附 录 B
（资料性附录）
共识机制相关数据格式

B.1 类拜占庭容错

注：类拜占庭容错共识算法是指能解决拜占庭将军问题的一类算法，典型的如 PBFT 算法及其演变的类似算法。

B.1.1 验证者格式

B.1.1.1 验证者地址

验证者地址的数据格式要求见表B.1。

表B.1

属性	内容
中文名称	验证者地址
英文名称	Validator Address
数据类型	字符串
数据长度	定长
数据说明	地址作为验证身份的标识，验证者不可更改其地址。
数据备注	可选

B.1.1.2 验证者公钥

验证者公钥的数据格式要求见表B.2。

表B.2

属性	内容
中文名称	验证者公钥
英文名称	Validator Public Key
数据类型	字符串
数据长度	定长
数据说明	验证者公钥用来验证验证者签名的正确与否，公钥编码后也可得到其相应验证者地址。
数据备注	必选

B.1.1.3 验证者投票权重

投票权重的数据格式要求见表B.3。

表B.3

属性	内容
中文名称	投票权重
英文名称	Validator Voting Power
数据类型	整数
数据长度	定长
数据说明	验证者根据所占投票权重进行投票，投票中超过一定比例的权重可进入下一轮投票。
数据备注	必选

B.1.2 验证者

B.1.2.1 验证者地址列表

验证者地址列表的数据格式要求见表B.4。

表B.4

属性	内容
中文名称	验证者地址列表
英文名称	Validator Address
数据类型	数组
数据长度	不定长
数据说明	验证者列表包含当前区块链系统里所有的验证者，验证者具有区块记账的权利。
数据备注	必选

B.1.2.2 提案者

提案者的数据格式要求见表B.5。

表B.5

属性	内容
中文名称	提案者
英文名称	Proposer
数据类型	数组
数据长度	定长
数据说明	提案者也是验证者，但相对验证者多了提交打包下一个区块提案的任务。
数据备注	必选

B.1.2.3 验证者投票权重总和

验证者投票权重总和的数据格式要求见表B.6。

表B.6

属性	内容
中文名称	权重总和
英文名称	Total Voting Power
数据类型	整数
数据长度	定长
数据说明	当前区块链系统里所有验证者投票权重的总和。
数据备注	必选

B.1.3 投票

B.1.3.1 投票者地址

投票者地址的数据格式要求见表B.7。

表B.7

属性	内容
中文名称	投票者地址
英文名称	Voter Address
数据类型	字符串
数据长度	定长
数据说明	地址作为投票者在区块链里的身份标识，地址由公钥编码后产生。
数据备注	必选

B.1.3.2 投票者序号

投票者序号的数据格式要求见表B.8。

表B.8

属性	内容
中文名称	投票者序号
英文名称	Voter Index
数据类型	整数
数据长度	定长
数据说明	投票者在投票者列表里会有唯一的序号作为投票者另一身份标识。
数据备注	可选

B.1.3.3 被投票的区块高度

被投票的区块高度的数据格式要求见表B.9。

表B.9

属性	内容
中文名称	投票高度
英文名称	Voting Height
数据类型	整数
数据长度	定长
数据说明	指准备打包的下一个区块的高度，即当前区块链的下一个区块高度。
数据备注	必选

B.1.3.4 投票轮次

投票轮次的数据格式要求见表B.10。

表B.10

属性	内容
中文名称	投票轮次
英文名称	Voting Round
数据类型	整数
数据长度	定长
数据说明	投票者所处轮次，在打包一个区块的过程中节点会经过多个轮数，每个轮数会有相应的时间限制。
数据备注	非可选

B.1.3.5 投票的类型

投票类型的数据格式要求见表B.11。

表B.11

属性	内容
中文名称	投票类型
英文名称	Voting Type
数据类型	整数
数据长度	定长
数据说明	在提交一个区块时，存在多种投票类型。这里用不同整数来表示具体的投票类型，如：预投票，预提交。
数据备注	非可选

B.1.3.6 投票区块标识

投票区块标识的数据格式要求见表B.12。

表B.12

属性	内容
中文名称	投票区块标识
英文名称	Voting Block ID
数据类型	字符串
数据长度	定长
数据说明	所投区块的摘要，此摘要通过区块的内容做哈希运算得到。
数据备注	必选

B.1.3.7 投票者签名

投票者签名的数据格式要求见表B.13。

表B.13

属性	内容
中文名称	投票者签名
英文名称	Signature
数据类型	字符串
数据长度	定长
数据说明	投票者对投票信息的签名，此签名可代表其所做动作确实是其所为，而非他人。
数据备注	必选

B.2 基于权益的证明

B.2.1 权益累计时长

权益累计时长的数据格式要求见表B.14。

表B.14

属性	内容
中文名称	权益累计时长
英文名称	Accumulated Stake Duration

属性	内容
数据类型	整数
数据长度	定长
数据说明	参与记账投票权益的时长，权益证明成功产生新的权益后，权益时间会清零。
数据备注	必选

B.3 基于工作量的证明

B.3.1 随机数

随机数的数据格式要求见表B. 15。

表B.15

属性	内容
中文名称	随机数
英文名称	Nonce
数据类型	整数
数据长度	定长
数据说明	基于工作量证明的区块链系统会要求记账者（矿工）找到适当的随机数，对该随机数和待记账的区块内容的合并信息进行Hash运算，并要求计算出来的Hash值必须满足特定格式（通常必须以特定数量的0开始）。
数据备注	必选

B.3.2 区块记账者

区块记账者的数据格式要求见表B. 16。

表B.16

属性	内容
中文名称	区块记账者
英文名称	Block Generator
数据类型	字符串
数据长度	定长
数据说明	标识实际提交本区块的记账者（矿工）信息，通常用记账者的公钥地址或账户地址来表示。
数据备注	必选

参考文献

[1] GB/T 18391.1-2002 信息技术 数据元的规范与标准化 第 1 部分 数据元的规范与标准化框架
[2] GB/T 18391.2-2009 信息技术 数据元的规范与标准化 第 2 部分 数据元的分类
[3] GB/T 18391.3-2001 信息技术 数据元的规范与标准化 第 3 部分 数据元的基本属性
[4] GB/T 18391.4-2001 信息技术 数据元的规范与标准化 第 4 部分 数据定义的编写规则与指南
[5] GB/T 18391.5-2001 信息技术 数据元的规范与标准化 第 5 部分 数据元的命名和标识原则
[6] CBD-Forum-001-2017 区块链 参考架构