ICS 35.020
I651

T/ SIA

中 国 软 件 行 业 协 会 团 体 标 准

T/SIA 007—2018

区块链平台基础技术要求

Blockchain Platform Basic Technical Requirements

2018-12-05 发布　　2018-12-05 实施

中 国 软 件 行 业 协 会 发布

目 录

前　言

本标准按照GB/T 1.1-2009 《标准化工作导则第1部分：标准的结构与编写》起草。

本标准主体部分包括总体要求、区块链数据、共识机制、加密机制、智能合约、账户管理、API及扩展能力。

本标准由中国软件行业协会提出并归口。

本标准起草单位：赛迪（青岛）区块链研究院有限公司、中国软件行业协会区块链分会、工业和信息化部计算机与微电子发展研究中心（中国软件评测中心）、北京天德科技有限公司、北京太一云科技有限公司、华为软件技术有限公司、苏州超块链信息科技有限公司、北京奇虎科技有限公司、北京信任度科技有限公司、齐鲁工业大学、深圳市前海微密网络技术有限公司、南京壹证通信息科技有限公司、上海分布信息科技有限公司、北京东软望海科技有限公司、广州广电运通金融电子股份有限公司、打零工(上海)互联网科技有限公司、北京筑龙信息技术有限责任公司。

本标准主要起草人：曾晋、刘权、崔志如、吕韬、万晨阳、黄忠义、曹兆磊、高睿、邹博松、赵华伟、姚一楠、聂春冰、郁莲、王炜、林冠辰、甘国华、陈光宇、张小军、吴英礼、任传伟、马臣云、许科峰、刘秋杉。

本标准为首次发布。

1 范围

本标准规定了区块链平台的基础技术要求，主要包括总体要求、区块链数据、共识机制、加密机制、智能合约、账户管理、API及扩展能力等方面。明确了区块链平台每项技术的定义及基础要求，对每项要求的具体实现方式不作规定。

2 规范性引用文件

本标准在编写时主要参考及引用了以下文件。凡是注日期的引用文件，仅注日期的版本适用于本文件；凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

CBD-Forum-001-2017 区块链-参考架构

CBD-Forum-002-2017 区块链-数据格式

可信区块链：第 1 部分 区块链技术参考框架

3 术语

3.1

区块链 blockchain

区块链是一个以区块为基本数据单元、按顺序储存的多副本的分布式存储技术。其中，区块是一段时间内的一组特定数据的集合，由区块头和区块体两部分组成；一般按顺序是根据区块产生的时间顺序，并且前后区块用密码技术保障顺序的安全性。区块链是分布式存储、共识机制、点对点通讯、密码算法等计算机技术在互联网时代的集成式创新和应用模式。

3.2

区块链平台 blockchain platform

实现区块链的信息化平台。

3.3

区块头 block header

区块头包含当前区块的属性信息和前一个区块顺序固定信息。属性信息包括当前区块的时间戳、区块序号等。前一个区块顺序固定信息，一般是用能唯一标识前一个区块特征的hash值代表。

3.4

区块体 block body

区块体是区块中存储数据的主要部分。存储的数据可以是一条或多条交易记录，也可以是一段可执行程序代码，或者是其他需要防止篡改的数据，如身份信息、资产信息等。

3.5

块链式数据结构 chained-block data structure

一段时间内发生的事务处理以区块为单位进行存储，并以密码学算法将区块按时间顺序连接成链条的一种数据结构。

3.6

共识机制 consensus mechanism

区块链系统中通过数学算法实现不同节点之间对记账内容达成一致的方法，是区块链系统确认状态，节点间建立信任、协同合作的基础。

3.7

Hash 函数 Hash function

又称摘要函数，通常通过特定数学计算将可变长度的信息输入变成可验证的唯一固定长度的短信息输出，用以唯一标识指定信息，可用于信息索引或保障数据的完整性。

3.8

非对称加密算法 asymmetric cryptographic algorithm

非对称加密算法亦称公钥加密算法。此类算法采用一对密钥：公钥和私钥一一对应，并且通过公钥难以计算出私钥。私钥应被拥有方秘密保存，用于计算数字签名，该签名可被对应的公钥验证；公钥需要公开发布，用于加密数据，且加密后的数据可被对应的私钥解密。

3.9

智能合约 smart contract

智能合约是以数字形式定义的能够自动执行条款的合约，通常是由一组特定的程序构成。智能合约通过账本管理交易，它们可以允许网络参与者自动执行交易的某些过程。当合约的条件满足时，合约将自动执行，执行结果将通过区块链的共识确认，并记录在区块链的分布式账本上。

3.10

用户 user

区块链的用户是指使用区块链产品或服务解决其业务问题的组织、个人或信息系统。

3.11

节点 node

区块链中代表用户利益参与记账的计算机或智能设备称为节点。节点保存着自己的一份或者部分账本，通过算力或者份额投票的方式来解决共识问题，通过无信任的方式确保全体节点遵循的账本和自己的账本是一致的。

4 总体要求

通常情况下，区块链平台应满足以下技术要求：

a）应基于某种算法提供链式数据结构（分布式账本），通过以区块为单位将一段时间内发生的事务进行储存；

b）应提供某种共识服务，通过算法验证可以将某种交易写入账本，必要时可以根据场景允许用户自主选择共识算法；

c）应提供针对许可链的身份管理和权限控制功能，如基于合约、用户、区块链等级别的权限管理，分级的权限控制；

d）应提供加密服务，支持主流加密算法，保障链上链下以及通信数据的安全性；

e）应提供智能合约服务，具有将数据管理逻辑、应用逻辑、业务规则和合同条款集成进分布式应用程序的能力；

f）应提供区块链管理平台和开发工具，包括用于编写、记录、测试、部署和监控分布式应用的工具SDK、API等。

5 区块链数据

5.1 数据结构

5.1.1 账本类应用数据结构

a）账本类应用数据结构是在区块链基本结构上面向账本设计而扩展出的数据结构，数据结构应能支持交易型计算收敛，能达成账本最终一致性；

b）账本类应用数据结构应包含交易发送方，交易接收方，交易金额，交易hash值；

c）账本类应用数据结构宜包含交易版本，交易标识，交易发送方公钥，交易发起者的私钥签名，交易数量，交易时间戳，对前置交易的引用；

d）账本类应用数据结构宜包含交易操作指令序列，指令序列长度，指令语言版本。

5.1.2 合约类应用数据结构

a)合约类应用数据结构是在区块链基本结构上面向事件触发计算型应用设计而扩展出的数据结构，数据结构应能支持事件触发的计算收敛，能达成计算结果最终一致性；

b)合约类应用数据结构应包含计算指令序列，计算结果，验证hash值；

c)合约类应用数据结构宜包含计算指令序列长度，指令序列版本，计算结果时间戳。

5.2 数据通信

a）应支持节点对节点通信；

b）应支持节点间安全通信，防止数据在传输途中被篡改，传输数据涉及个人信息，应遵守国家个人信息保护相关规范，进行加密传输；

c）节点通信宜提供多播能力；

d）区块链平台宜提供跨区块链互操作性标准，提供跨链资产和信息的交互服务。

5.3 数据存储

a）应支持按照一定的算法进行全部节点或部分节点的区块数据同步；

b）不同节点存储的区块数据应能保持完整性；

c）涉及个人信息等敏感信息的数据，在存储时应遵守国家个人信息保护相关规范，进行加密存储；

d）节点宜提供独立的、完整的数据存储。

5.4 数据处理

a）区块链平台应披露网络及系统的配置信息，包括区块配置方式，网络环境，共识机制等；

b）应能满足指定业务场景的数据处理效率，例如交易数据的处理，账户的创建，导出，导入，映射等。

5.5 数据同步

a）新增节点应能同步全部或部分链上信息，且满足区块链平台声明的效率要求；
b）所有参与共识验证的节点在进行同步时应具有较高的效率。

6 共识机制

6.1 共识算法

a）共识算法应能够在参与共识的节点互不信任的基础上达成共识；
b）共识算法应公开技术细节；
c）共识算法应支持节点独立进行算法运算，不依赖任何其他节点数据和状态；
d）共识算法应保证各节点对上链数据打包区块的计算能收敛并达到最终一致性；
e）共识算法应声明在一定规模的节点环境下达成共识所需的理论时间；
f）应有明确的抗恶意攻击指标；
g）共识算法宜提供算法版本配置管理机制。

6.2 共识容错

a）应保证当任意不超过区块链平台声明数量的节点发生故障，整个系统工作正常；
b）应能抵御重放攻击，网络上任意节点获取用户请求消息之后，重放会执行失败；
c）应提供防止消息篡改的验证机制。

6.3 共识效率

a）应声明与共识相关的效率指标，如：吞吐量，并发数，响应时间，算力消耗等；
b）区块链平台的共识效率应能满足指定业务场景的要求。

7 加密机制

7.1 加密算法

a）区块链平台宜符合国家密码管理相关规范；
b）区块链平台宜采用对称和非对称结合的混合加密机制；
c）私钥应在用户本地生成并保存，私钥的储存应符合国家个人信息保护相关规范；
d）私钥的使用宜采用双因素或多因素认证。

7.2 隐私保护

a）用户的身份和事务处理等信息不得在区块链产品中明文传输、存储；
b）应对用户数据的访问采用权限控制；
c）宜阐明隐私保护的范围和目标；
d）宜阐明第三方验证的手段。

8 智能合约

8.1 智能合约机制

a）区块链平台应添加智能合约机制，向用户提供可靠高效的智能合约服务；
b）应提供智能合约运行的载体，如虚拟机等；
c）宜支持多方共识下的合约升级功能。

8.2 智能合约安全性

a）智能合约执行的环境宜与网络、文件系统或者其它进程隔离，代码执行仅限合约范围内；

b）智能合约环境宜具有一定程度的代码审查功能，防止代码缺陷引发的安全隐患；

c）应检查外部调用函数的安全性；

d）智能合约应包含容错和异常终止功能，同时具有运行时间及资源占用可控性。

9 账户管理

9.1 账户权限

a）区块链平台应声明账户标识机制；

b）区块链平台应声明账户的验证与证明机制，包括语法与格式、验证与证明机制；

c）区块链平台应声明账户的鉴别机制，例如密钥、生物识别、等级等；

d）区块链平台应声明账户的授权机制，例如基于角色、密码、属性等；

e）区块链平台应声明账户的集成应用与身份管理机制。

9.2 账户功能

a）区块链平台应提供基本的账户注册、地址生成等功能；

b）区块链平台应提供明确的账户登入登出方式；

c）区块链平台应提供基本的账户更新、注销功能；

d）区块链平台应提供基本的账户告警和异常应对功能；

e）区块链平台应提供基本的账户信息查询功能；

f）区块链平台应提供基本的账户管理功能，包括密钥管理方式。

9.3 身份可信

a）应提供统一的账户管理服务系统，保证注册用户身份的真实性；

b）宜通过自身建设或作为已有CA系统的代理提供统一的CA认证服务系统，实现签发各类数字证书，并保证网络接入和交易用户的身份真实性。

9.4 CA（证书认证中心）的支持表

区块链平台系统宜能够通过SDK或远程过程调用(RPC，RESTFul)提供以下CA认证相关服务：

a）用户注册接口：实现用户账号的注册和密码设置；

b）用户登录接口：实现用户账号与密码的验证；

c）实名认证接口：实现用户身份信息真实有效性的验证与识别；

d）用户注销接口：实现用户账户信息注销和相关证书的作废；

e）获取CA根证书接口：登录与实名认证通过后，用户获取CA服务的Root证书；

f）申请接入证书接口：向CA服务申请用户节点接入证书；

g）申请交易证书接口：向CA服务申请用户交易验证证书；

h）证书作废接口：向CA服务发起证书作废请求，完成证书作废操作；

i）证书状态查询接口：向CA服务发起证书信息查询，获取证书相关信息。

10 API 及扩展能力

a）区块链平台应做好API接口的权限控制，避免非授权调用；

b）区块链平台接口调用方式应支持SDK，或者远程过程调用（RPC，RESTful）。

c）区块链平台应提供以下接口以处理与交易、区块相关的业务：创建业务表接口、交易发送接口、查询交易接口、查询块接口、创建索引接口；

d）区块链平台应提供以下接口以处理智能合约相关的业务：创建智能合约接口、智能合约上链（部署）接口、智能合约执行接口、结果查询接口、创建索引接口。