ICS 35.240
CCS L 70

DB51

四 川 省 地 方 标 准

DB51/T 3189—2024

区块链技术应用规范

2024－10－08 发布　　2024－11－08 实施

四川省市场监督管理局　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由四川省发展和改革委员会提出、解释、归口并组织实施。

本文件起草单位：电子科技大学、四川省大数据中心、迅鳐成都科技有限公司、成都市标准化研究院、四川省卫生信息学会、四川省司法厅、四川省生态环境厅、四川省医疗保障局、成都市教育局、成都市医疗保障局、国家信息中心、德阳市政务服务和大数据管理局、内江市大数据中心、中国核动力研究设计院、四川省特种设备检验研究院、北京工业大学、成都市智慧蓉城研究院有限公司、华为技术有限公司、四川省计算机研究院、成都城投教育投资管理集团有限公司、四川华西集采电子商务有限公司、联通（四川）产业互联网公司、四川省电子信息产业技术研究院有限公司、四川通信科研规划设计有限责任公司、成都武侯社区科技有限公司、亚信科技（中国）有限公司、成都飞机工业（集团）有限责任公司、成都交子区块链产业创新中心有限公司、成都中医药大学、国信优易数据股份有限公司、国信优易（北京）数据要素科技有限公司、福建省数易科技有限公司、四川网道科技发展有限公司、四川迅鳐科技有限公司、四川省大数据发展研究会。

本文件主要起草人：夏琦、周学立、高建彬、夏虎、祝玲、管庆旭、张军、段占祺、段莹、刘雯、乐益矣、丁云波、曾子敬、戴子玟、周云宏、王平、温蓓、刘易飞、张心玥、李蒙科、冯暄、赵斌、邓忆德、高会伟、王旭赢、刘莎、盛杰、阳丽文、陈睿、徐斌、尹嘉奇、罗英、李亚军、单志广、郭煜、林晓东、向海平、明子涵、李健、董雪璠、肖丽、王楠、才虹丽、秦强子、周书田、郭凯、封博文、王少巍、张远民、陈伟、欧阳森山、廖丹、王亚松、王贝贝、李弋凡、阮亚芬、吕一新、马丹、陈国平、申林、陈华、李莹珠、杜翔、陈庆、王越、李子欣、王鹏、李依婷、程捷、高然、白玲玉。

区块链技术应用规范

1 范围

本文件规定了四川省区块链技术应用规范，主要包括区块链应用架构、应用基础设施层建设要求、基础资源层基本要求、应用支撑层基本要求、分布式应用层基本要求、应用安全保障体系要求等。

本文件适用于指导四川省区块链平台每项技术的基础应用要求，对每项要求的具体实现方式不作规定。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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。

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 25069—2022 信息安全技术 术语

GB/T 42752—2023 区块链和分布式记账技术 参考架构

3 术语和定义

下列术语和定义适用于本文件。

3.1

账户数据 account data

描述区块链事务的实际发起者的相关数据，使区块中记录的事务信息能被有效关联。

3.2

区块数据 block data

由零个或多个交易记录或对交易记录的引用组成的结构化数据。

[来源：ISO 22739：2020，3.3]

3.3

区块链 blockchain

使用密码技术链接将共识确认过的区块按顺序追加形成的分布式账本。

注：区块链被设计用来抵抗篡改，并创建最终的、确定的、不可变的账本记录。

[来源：ISO 22739：2020，3.6]

3.4

共识算法 consensus algorithm

区块链系统中各节点为达成并维护系统数据一致性的计算方法。

注：常见共识算法有工作量证明（Proof of Work，PoW）算法、权益证明（Proof of Stake，PoS）算法、股份授权证明（Delegated Proof of Stake，DPoS）算法、实用拜占庭容错（Practical Byzantine Fault Tolerance，PBFT）算法。

3.5

配置数据 configuration data

区块链网络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。

3.6

密码链接 cryptographic link

使用密码散列函数技术构造的、指向数据的引用。

注：区块头中使用密码链接来引用前一个区块，以创建仅可追加的、有序的链，从而形成区块链。

[来源：ISO 22739：2020，3.16]

3.7

跨链适配器 cross chain adapter

操作特定区块链的网络组件，用来调用区块链上的智能合约，以及对跨链交易指令及交易结果进行验证。

3.8

跨链可信通道 cross chain trusted channel

连接不同区块链与统一许可联盟链网的网络节点，实现跨链交互信息的传递及转换，参与跨链交易安全认证及有效性共识。

3.9

分布式数字身份文档 decentralized identity document

用于登记和验证个体的身份信息，包括身份标识符、加密密钥、验证方式和服务端点等，以支持安全的身份验证和数据交换的数据记录。

3.10

分布式应用 distributed application

使用开放分布式系统中的两个或更多个应用实体调用来完成信息处理。

3.11

分布式账本 distributed ledger

在一组分布式记账技术节点之间共享并使用共识机制同步的账本。

注：分布式账本被设计为防篡改、仅可追加和不可变，包含确认和验证的交易。

[来源：ISO 22739：2020，3.22]

3.12

数字签名 digital signature

附加在数据单元上的数据，或是对数据单元做的密码变换，这种数据或变换被数据单元的接受者用以确认数据单元的来源和完整性，并保护数据防止被人（例如接收者）伪造或抵赖。

[来源：GB/T 25069—2022，3.576]

3.13

联盟链 consortium blockchain

由若干个机构或者组织共同参与管理的区块链，每个参与的机构或者组织都运行着里面的一个或多个节点，其中的数据只允许系统内不同的机构进行读写和发送交易，并且共同来记录交易数据。

3.14

账本记录 ledger record

分布式账本上的记录，包含交易记录、交易记录的哈希值和交易记录的引用。

注：引用可以实现为密码链接。

[来源：ISO 22739：2020，3.44]

3.15

许可联盟链网 license alliance chain network

采用联盟区块链系统设计，附带区块链的身份管理、隐私保护等安全特点，作为跨链体系的核心，统筹管理跨链事务。

3.16

私有链 private blockchain

区块链的写入权由某个组织或者机构控制的区块链，参与到区块链的节点会被严格限制起来。

3.17

公有链 public blockchain

全世界任何人都可读取、发送交易且交易能获得有效确认的、也可以参与其中共识过程的区块链。

注：公有链完全是去中心化的存在，不受任何组织或者机构掌控。

3.18

合约数据 contract data

描述事务的动态处理逻辑的数据,实际是可在虚拟机上执行的一段计算机代码。合约又称智能合约。

3.19

身份存储库 identity hub

能够去中心化地控制用户个人敏感数据，支持链下存储和授权访问，且兼容本地和云端部署的隐私数据系统。

3.20

运行时服务 runtime service

为中间件提供运行环境，负责系统内部数据与流程的解释与定义，对外提供接口调用的服务组件。

3.21

智能合约 smart contract

存储在分布式记账技术系统中的计算机程序，该程序的任何执行结果都记录在分布式账本上。

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。

[来源：ISO 22739：2020，3.72]

3.22

交易数据 transaction data

描述区块链网络承载的具体业务动作的数据。通常包括业务逻辑执行结果和交易转账信息等。

4 缩略语

下列缩略语适用于本文件。

API：应用程序接口（Application Programming Interface）

CCIP：跨链交互协议（Cross Chain Interaction Protocol）

CPU：中央处理器（Central Processing Unit）

DES：一种对称加密算法（Data Encryption Standard）

DID：分布式数字身份（Decentralized Identity）

ID：身份标识符（Identity Identifier）

I/O：计算机接口，输入/输出（Input/Output ）

P2P：点对点（Peer to Peer）

PC：个人电脑（Personal Computer）

RPC：远程过程调用（Remote Procedure Call）

RSA：公钥加密算法（“Rivest－Shamir－Adleman”Algorithm）
SAS：串行SCSI（Serial Attached SCSI）
SATA：串行硬件驱动器接口（Serial Advanced Technology Attachment）
SCSI：Internet小型计算机系统接口（Internet Small Computer System Interface）
SDK：软件开发工具包（Software Development Kit）
SHA256：256位安全哈希算法（Secure Hash Algorithm 256-bit）
SM2：椭圆曲线公钥密码算法（Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves ）
SM3：密码杂凑算法（SM3 Cryptographic Hash Algorithm ）
SM4：分组密码算法（SM4 Block Cipher Algorithm ）
SSD：固态硬盘(Solid State Disk)
USB：通用串行总线（Universal Serial Bus）
VC：可验证声明（Verifiable Claim）

5 区块链应用架构

5.1 总体架构

为了便于分析与规范说明，本规范基于区块链技术特点，对区块链技术进行了四层的架构划分以及提供区块链应用安全保障体系。四层架构分别为基础设施层、基础资源层、应用支撑层、分布式应用层，总体架构如图1所示。

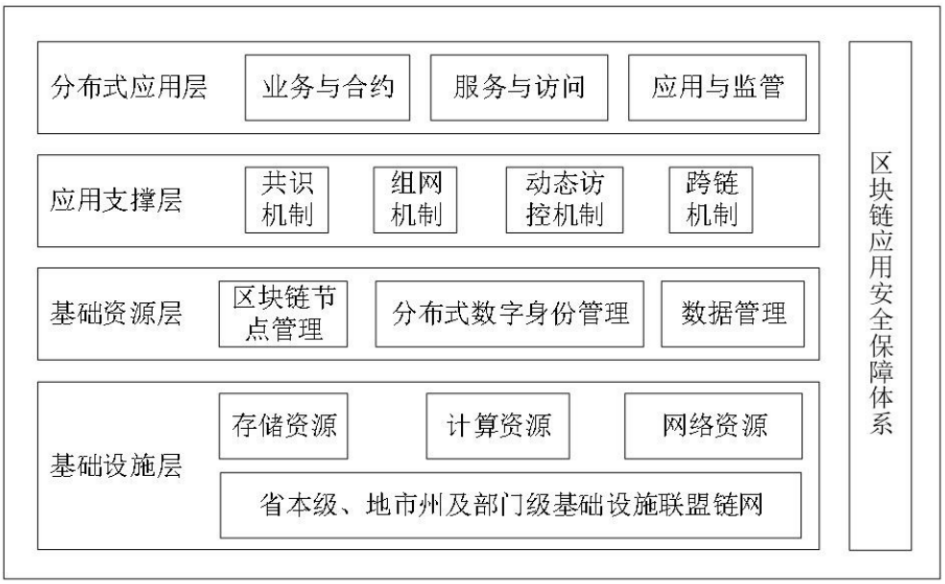

图1 四川省区块链应用总体架构图

5.2 架构说明

总体架构说明如下：

a) 基础设施层：构建了一个由基础设施联盟链网支撑的应用环境，通过提供存储、计算和网络资源，为上层应用奠定坚实基础；

b) 基础资源层：基于基础设施层提供的硬件和网络基础体系，提供核心功能支撑，包括区块链节点管理、分布式数字身份和数据管理，确保业务逻辑与监管需求的融合，为应用支撑层提供相应的功能支持服务；
c) 应用支撑层：提供组网、共识、动态访问和跨链机制等功能，促进数据流通与访问控制；
d) 分布式应用层：通过调用应用支撑层的功能组件，提供多元化的服务和访问能力，支持丰富的分布式应用开发与部署，形成一个完整、高效、安全的区块链应用生态系统；
e) 区块链应用安全保障体系：针对区块链应用面临的安全风险，对区块链基础设施层、基础资源层、应用支撑层、分布式应用层提出相应的技术安全要求。

6 区块链应用基础设施层建设要求

6.1 基本要求

基础设施层主要包括存储资源、计算资源、网络资源、省本级、地市州及部门级基础设施协同链网涉及的跨链网络建设，该部分均要求基于国产自主可控技术实现。

6.2 存储资源

6.2.1 存储资源提供区块链运行过程中产生的各种类型数据，如账本、交易信息等的写入及查询功能，相关选型包括但不限于关系型数据库、键值对数据库、文件数据库等。

6.2.2 存储资源应满足以下需求：

——点对点网络中，能够被每个节点部署并使用；

——能够高效、安全、稳定地提供数据写入及查询服务；

——对于采取分库分表的数据存储方案，存储资源还应包括数据的分片及路由处理能力。

6.2.3 存储基础设施应采用分布式架构，提供可弹性扩展的虚拟化存储硬盘。同时，存储硬盘应具有高数据可靠性，高 I/O 吞吐能力，根据不同的应用场景，支持 SATA、SAS、SSD 等多种存储介质。

6.2.4 为保障存储多样性，存储基础设施需提供块存储、文件存储、对象存储等多种存储模式。

6.2.5 为保障系统安全可靠，存储设备需采用国产化自主可控芯片。

6.3 网络资源

6.3.1 区块链系统运行的底层拓扑结构是分布式对等网络，应采用对等网络协议组织区块链中的各个网络节点。

6.3.2 各个节点间通常使用点对点通信协议完成信息交换以支撑上层功能。

6.3.3 网络传输资源通常应满足以下需求：

——能够进行点对点之间的高效安全通信；

——能够提供点对点通信基础上的多播能力；

——应支持对节点的动态添加、减少的识别。

6.3.4 系统可实现网络自动化部署，支持灵活弹性、业务动态变化。

6.3.5 系统可实现大规模的租户网络隔离，互不干扰，各租户可提供独立的网络服务。

6.4 计算资源

6.4.1 计算资源提供区块链系统运行中的计算能力支持，包括但不限于物理机技术、虚拟机技术、云计算技术等。

6.4.2 计算机资源应满足以下需求：

——对区块链系统提供运行环境支持；

——点对点网络中，能够被每个节点采用。

6.4.3 计算平台可以分钟级发放虚拟机设备，且这些基础设施是弹性的，可以根据需求进行扩展和收缩。为了保证虚拟机的可靠性，在发生服务器异常故障时，应使故障服务器上的虚拟机在其它服务器通过双机集群功能运行起来。

6.4.4 为保障系统安全可靠，服务器设备应采用国产化自主可控设备。

6.5 省本级、地市州及部门级基础设施许可联盟链网建设要求

6.5.1 基础设施许可联盟链网部署架构图

省本级、地市州及部门级基础设施许可联盟链网部署架构如图2所示。

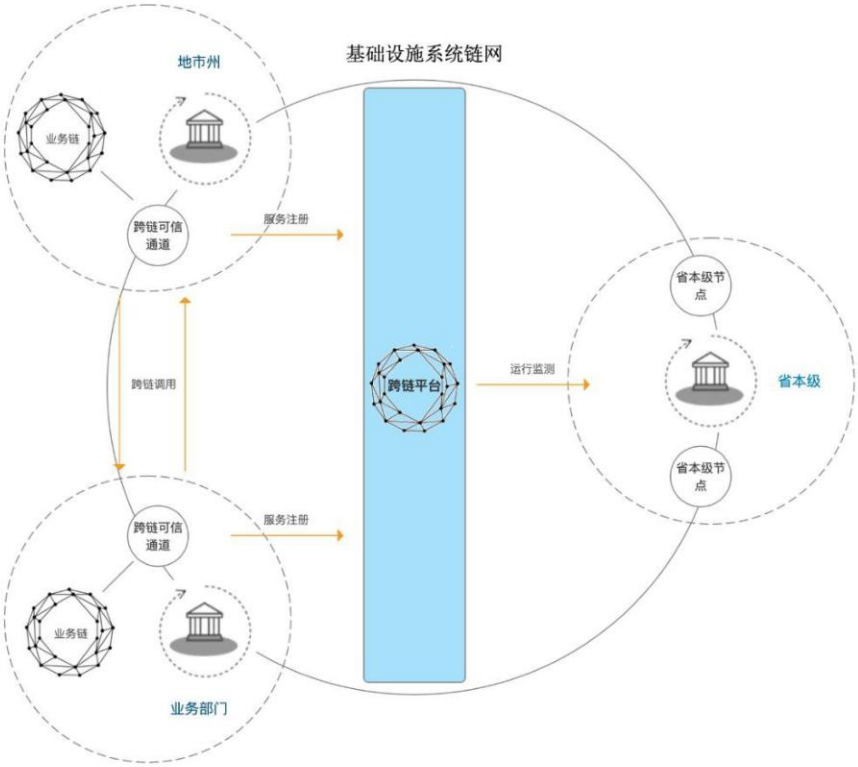

图2 基础设施许可联盟链网部署架构图

6.5.2 跨链机制应用要求

6.5.2.1 应支持基于中继链、公证人、双向锚定等技术的基础设施协同跨链网络。

6.5.2.2 应支持基于不同区块链内核所构建的同构及异构链之间的互联互通，打破区块链数据孤岛，助力不同联盟链可信互联，促进区块链产业生态可信融合。

6.5.2.3 应支持跨链申请、授权等操作行为完整保存上链，交易过程记录本地账本，全流程自动、透明、可监督，支持事中校验、事后审计，保障多方权益。

6.5.2.4 应支持跨链账本数据以及智能合约数据仅在所有者授权情况下才能进行访问，基于身份体系对跨链合约及账本查询和交易操作提供授权能力，在保护数据安全的同时，还保证数据的使用过程可以被追溯。

6.5.2.5 应支持基于分布式身份体系的跨链系统治理，为各个接入的区块链配置通用身份标识，支持基于标识寻址发起跨链访问。

6.5.2.6 应支持跨链事务一致性要求，包括：保障跨链交易在整个流程中的事务一致性；支持事务超时处理机制，在事务超时且不满足一致性要求时进行回滚处理；支持实时或周期性的事务检查机制。允许事务回滚失败时，通过第三方介入的方式保障事务一致性。

6.5.2.7 应支持跨链可靠性和可用性要求，包括：

——应支持链间互操作组件出现故障后自动回滚；

——应支持无单节点故障，可采用多活或负载均衡方式；

——应支持跨链事务数据和配置的自动备份；

——应支持数据备份，并支持利用备份数据在系统故障时快速恢复业务环境；

——应支持账本增量或全量备份；链间互操作组件宜支持账本备份，可以为其他节点恢复数据。

6.5.2.8 应支持跨链隐私保护能力，保证跨链交互数据安全可靠，跨链中继不记录对应链的数据信息，支持跨链组件点对点数据交互，防止隐私泄露，有效保护跨链数据隐私。

6.5.2.9 应支持跨链接入安全要求，包括：

——应支持通过用户数字证书进行身份认证；

——应支持超时断开机制，超时后应断开用户会话或重新鉴别用户身份；

——应支持在用户认证失败达到指定次数后，阻止用户再次发起认证请求；

——宜支持动态口令卡、USB Key、指纹、智能卡认证进行身份认证，其配套设备和系统必须符合国家相关规定；宜支持双因子认证。

6.5.2.10 应支持跨链数据传输和存储安全，包括：

——支持跨链交易端到端的完整性保护；

——支持跨链通信端到端传输过程中的加密保护；

——支持链间互操作组件账本本地数据的加密存储；

——跨链交易数据只能被目的方获取，其它方无法获取；

——支持区块链中的非授权数据无法被链间互操作组件访问。

6.5.3 跨链接入要点

6.5.3.1 跨链初始配置要点应包括：

——宜在接入机构建设跨链可信通道，为跨链可信通道配置与其他通道联通的网络环境，以在不同机构间构建互通跨链网络；

——跨链适配器部署于跨链可信通道内，宜通过跨链适配器连接接入机构的本地业务区块链网络；

——接入机构应进行身份注册，并为其分配用于跨链交互时验证身份的密钥或证书等。

6.5.3.2 跨链网络接入要点包括接入机构的跨链可信通道、跨链适配器、本地业务区块链网络均需进行注册，生成相应的唯一标识符。

6.5.3.3 业务区块链监测要点包括接入机构业务区块链的基本情况、运行状态进行监测，应及时反映整个跨链网络的运行情况。

7 区块链基础资源层基本要求

7.1 区块链节点管理

7.1.1 共识/记账节点

7.1.1.1 区块链节点应包括共识节点和记账节点，应提供管理平台对节点进行配置，节点服务启动时根据配置定义共识与记账节点。
7.1.1.2 区块链节点根据配置定义为共识节点，应提供合约容器部署功能，提供共识机制，提供记账功能。
7.1.1.3 区块链节点根据配置定义为记账节点，仅提供记账功能。

7.1.2 签名验签机制

7.1.2.1 区块链节点应根据配置的算法与证书验证节点间、APP、合约等通信。
7.1.2.2 区块链节点应根据配置算法与证书做数据签名。

7.1.3 加密组件库

7.1.3.1 区块链节点应支持多密码体系并行，加强数据安全、通讯安全。
7.1.3.2 区块链节点应利用账本分离、数据加密授权访问等加强隐私保护。
7.1.3.3 区块链节点应采用加密和认证对接入消息的客户端进行认证。
7.1.3.4 区块链节点宜支持 RSA 算法和国产 SM2 算法进行签名和验签，宜支持分组密码算法国际 DES、国产 SM4，SM3 杂凑算法 SHA256，ED25519 签名算法。

7.1.4 区块/区块链

应提供交易打包落地形成区块并按规则生成区块链功能。

7.1.5 Docker 服务

宜提供Docker服务在共识节点上部署合约容器，提供合约容器部署、删除、重命名等功能。

7.1.6 交易/交易池

7.1.6.1 区块链节点调用合约生成交易，交易缓存到交易池，当规则条件满足，打包形成区块。
7.1.6.2 宜提供交易池规则设定功能。
7.1.6.3 应通过合约执行产生读写集生成交易。

7.1.7 组网服务组件

区块链节点通过初始化组网服务组建区块链网络并运行，宜提供区块链节点更新服务、创世块执行服务、gRPC通信服务、gossip网络服务、Leader选举服务等。

7.2 分布式数字身份管理

7.2.1 DID 标识符

分布式数字身份应支持使用DID标识符作为一个身份的唯一识别信息。

7.2.2 DID 文档

一个DID标识符应对应一个DID文档（DID Document），DID文档数据应包含的数据元素见表1。

表1 DID 文档

数据元素	是否必选
DID 标识符	必选
加密材料集合（如公钥）	必选
数据元素	是否必选
验证方法集合	非必选
服务端点集合	非必选
创建时间	非必选
更新时间	非必选

7.2.3 DID 解析器

DID解析器应通过DID标识符来获取DID文档。

7.2.4 可验证声明

可验证声明数据应包含的数据元素见表2。

表2 可验证声明

数据元素	是否必选
VC 的 ID	必选
VC 发行者	非必选
声明的主体内容	非必选
声明的证明	非必选
发行时间	非必选

7.2.5 身份储存库

用户的隐私数据应使用身份存储库（Identity Hub）存储，且应满足以下要求：

——身份存储库应支持去中心化和链下方式的个人数据存储，应将个人数据的控制权交给用户，应支持用户以安全而隐私的方式存储其敏感数据，应用支持用户数据的授权访问；

——身份存储库应支持本地（包括手机、PC）或云端方式。

7.3 数据管理

7.3.1 数据结构

区块链技术相关的数据对象结构应包括区块、事务、实体、合约、账户、配置六个主要的数据对象。其中区块链核心数据对象包括区块、事务、实体和合约。具体各数据结构要求包括：

——区块链的账户数据应包含但不限于的数据元素见表 3；

表3　区块链账户数据

数据元素	是否必选
账户公钥	必选
账户私钥	必选
账户标识	非必选
账户资产	非必选
数字证书	非必选
账户所属机构	非必选

——区块链的区块数据应包含但不限于的数据元素见表 4；

表4　区块链区块数据

数据元素	是否必选
区块高度	必选
区块标识	必选
版本信息	非必选
前一区块摘要值	必选
默克尔树根	事务树根必选
区块时间戳	必选
区块随机数	非必选
难度系数	非必选
事务列表	非必选

——区块链的事务数据可包含但不限于的数据元素见表 5；

表5　区块链事务数据

数据元素	是否必选
事务标识	必选
事务类型	必选
签名者	必选
事务时间戳	必选

——区块链的实体数据应包含的数据元素见表 6；

表6　区块链实体数据

数据元素	是否必选
发起方地址	必选
接收方地址	必选
事务处理发生额	非必选
事务处理费用	非必选
存储数据	非必选
附件数据	非必选
实体数据备注	非必选

——区块链的合约数据可包含但不限于的数据元素见表 7；

表7　区块链合约数据

数据元素	是否必选
合约标识	必选
合约版本号	必选
合约代码	必选
合约存储	必选
合约所有者	必选

——区块链的配置数据应包含但不限于的数据元素见表 8。

表8　区块链配置数据

数据元素	是否必选
协议版本号	非必选
版本软件号	必选
节点标识	必选
节点地址	必选
节点公钥	非必选

7.3.2　数据通信

区块链的数据通信应具有的能力包括：

——支持 P2P 通信；
——支持节点间安全通信，防止数据在传输途中被篡改；
——数据传输连接建立之前对发送方和接收方进行身份鉴别的能力；
——数据传输应采用统一时间标准，具备对传输数据的可用性进行检测的能力；
——支持节点间数据传输的完整性验证；
——节点通信提供数据广播的能力。

7.3.3 数据存储

区块链的数据存储应具有以下能力：
——节点数据应具备加密存储能力；
——支持全节点，提供独立的、完整的数据存储能力；
——宜提供批量数据从链上下载到本地数据库的服务；
——宜提供区块链浏览器，上链数据的数据查找、定位、统计功能；宜提供数据本地化浏览服务；
——需支持设置用户访问权限，数据信息应进行安全保护分级；
——需具备一定容灾性功能，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。

7.3.4 数据处理

区块链的数据处理应具有以下能力：
——需具备披露网络及系统的配置信息的功能，包括区块配置方式，网络环境、共识机制等；
——需满足指定业务场景的数据处理效率指标，例如交易数据和账户的处理；
——需符合共识机制对数据的处理标准流程，包括事务接收、事务执行、事务打包、事务验证和事务提交；
——需具备现实数据映射上链应进行标准化处理和合法性验证的功能；
——宜支持从约定的信息系统或特定的数据来源渠道直接抽取或智能化采集等方式，对约定上链的数据进行采集或提取，约定上链的数据必须是真实和准确的；
——宜支持提供数据目录的发布、更新等数据目录服务；
——宜支持按区块链系统要求提供数据发布服务；
——宜提供批量数据上载发布服务功能。

7.3.5 数据同步

区块链的数据同步应具有以下能力：
——需支持对全部节点或部分节点按照一定的算法同步区块数据；
——新增节点应能同步全部或部分链上信息时，需满足区块链平台声明的效率要求；
——所有参与共识验证的节点在进行同步时应达到要求的最低效率指标；
——轻节点通过全节点进行数据同步流程应只同步关联账户数据；
——数据同步内容宜包括但不限于区块数据结构内容，根据业务需求和所负职责确定具体需要同步的内容；
——需符合数据同步处理方式和流程：区块将区块内容推送给区块链网络内的其他节点时采用广播推送式，向其他记账节点进行数据同步采用消息订阅式；
——区块链数据同步宜采用能减少账本数据的重建工作的技术或技术方案来增加同步效率；
——数据同步宜采用设定系统的区块数量自动检测点、多方参与状态数据恢复等技术方式使同步过程具备高可靠性；

——区块链账本数据同步能力需为各个区块链引擎必备的基本能力。

8 区块链应用支撑层基本要求

8.1 共识机制

8.1.1 共识达成的标准流程

8.1.1.1 共识机制要素

共识机制要素应包括：
——达成一致：机制将收集群体中所有一致意见；
——合作：群体中每个个体都是为了达成一致，从而群体利益一致；
——权利平等：群体中每个个体参与者都有相同的竞争权利；
——参与：群体中每个个体都需要参与；
——积极性：群体中每个个体具有相同的活跃度。

8.1.1.2 共识机制流程

共识机制流程应包括：

a) 加入共识：这个阶段决定哪些节点可以参与共识，缩小参与共识的节点范围。比如在 PoS 里面，则是需要持有代币或者交保证金才能参与共识。在 DPoS 里面，代理人需要获得足够多的投票才能参与共识；
b) 生成区块：采用共识算法（一定规则）从参与共识的节点里挑选相应的节点，由该节点将交易打包生成新的区块；
c) 进行验证和投票，节点验证更新区块。投票涉及区块投票和用消息投票两种方式，每个区块都是一张票（票有权重，例如工作量证明），高度最长、包含的区块（票数）最多即为胜出的链。

8.1.2 共识机制应用要点

区块链共识算法应用要点见表9。

表9 区块链共识算法应用要点

共识机制算法		应用要点
工作量证明类共识机制	Proof-of-Work 工作量证明	(1) 应将区块头数据带入哈希函数计算公式； (2) 应不断调整区块头数据中的随机数； (3) 应计算出满足特定标准的哈希值完成工作量证明。

表 9　区块链共识算法应用要点（续）

共识机制算法		应用要点
	Proof-of-Capacity 容量证明	(1) 用于规范区块链上新区块的验证； (2) 更多关注内存而不是处理能力； (3) 将工作量证明机制中的算力资源替换为磁盘空间资源，矿工之间通过比拼磁盘空间大小来竞争最后的记账权。
	Proof-of-Stake 权益证明	(1) 节点通过“抵押”一定数量的加密货币来参与区块的验证； (2) 获得新区块记账权的概率与验证者持有的代币数量成正比； (3) 引入了惩罚机制，如果验证者被发现进行不当行为（如双重支付攻击），其抵押的加密货币会被部分或全部没收（称为“Slashing”）。
	Delegated Proof-of-Stake 委托权益证明	(1) 通过投票选举出一定数量的代表来达成共识； (2) 所有节点都可以自主选择投票的对象，选举产生的代表按顺序记账。
	Proof-of-Weight 权重证明	(1) 在 PoS 中用户所拥有的网络中令牌的百分比，表示了该用户“发现”下一个区块的概率； (2) 权重证明使用了完全不同的加权值。
其他类共识机制	Practical Byzantine Fault Tolerance 实用拜占庭容错	(1) 该共识机制允许拜占庭容错，允许强监督节点参与，具备权限分级能力； (2) 所有节点都在相同的配置下运行，且有一个主节点，其他节点作为备份节点。
	Proof-of-Identity 身份证明	(1) 将用户的私钥与授权的身份进行比较； (2) 用户私钥的一段加密证据，该私钥以加密方式附加到特定的交易中； (3) 身份证明确保创建的数据的完整性和真实性。
	Replication and Fault Tolerant 基于领导者驱动的共识模型	(1) Raft 共识模块中使用心跳机制来触发 Leader 选举； (2) 领导者负责将日志复制到关注者。它通过发送心跳消息定期通知追随者它的存在； (3) 每个跟随者都有一个超时时间，它期望领导者的心跳，接收心跳时重置超时时间； (4) 如果没有收到心跳，则关注者将其状态更改为候选人并开始领导选举。
	Directed Acyclic Graphs 有向无环图	(1) 共识机制中，有向无环图将最长链共识改成最重链共识； (2) 新单元的发布会加入在原先的最长链之上，并且所有节点认为最长链为真，依次无限蔓延。

8.1.3　共识算法技术要求

8.1.3.1　去中心化

计算机网络中没有中心节点，所有节点地位相同，应满足以下要求：

——共识结果随机且概率相等；
——可以解决双花问题；
——可以解决拜占庭将军问题。

8.1.3.2 成本消耗

业务应用共识应计算共识过程中耗费的CPU、内存、网络资源与电力消耗等资源，并减少共识机制对等待中的交易进行哈希运算和校验的过程需要消耗的资源，吞吐量应满足应用场景的实际峰值需求。

8.1.3.3 可扩展性

可扩展性应包括：
——系统成员数量增加的可扩展性；
——待确认交易数量增加的可扩展性。

8.1.3.4 交易确认速度

业务应用共识应考虑系统每秒可处理确认的交易数量，满足应用场景的实际峰值需求。可通过以下方案解决：
——增加区块大小；
——实现链下交易；
——代理人共识协议解决方案。

8.1.3.5 容错能力与安全机制

业务应用共识应具备一定的容错性,包括节点发生物理或网络故障的非恶意错误和节点遭受非法控制的恶意错误，以及节点产生不确定行为的不可控错误。

8.1.3.6 共识机制算法最优化

根据区块链的现实情况中的节点数量、信任度分级、容错性、性能效率等指标，应灵活选择某种共识机制算法或对几种算法进行组合使用，以达到共识算法最优化，应满足以下要求：
——公有链情景下，所有节点拥有平等的权力并且引入代币激励机制，选择容错性较高且具有代币激励机制的算法；
——联盟链情景下，网络节点规模可控，内部存在不对等信任的节点，应选择容算性与性能效率适中、无需代币的算法。

8.2 组网机制

区块链组网应满足以下要求：
——应支持局域网、因特网、混合网络、移动网络、物联网等制式下的网络标识机制；
——应支持自组网功能；
——应支持网络运维服务，包括网络整体运行状态、网络节点状态与、网络拓扑、服务器性能监测等功能；
——应支持大规模节点自组网环境运行，支持账本高速同步的 P2P 网络；
——宜支持基于通道、gRPC 通信、Gossip 协议的数据同步。

8.3 动态访问控制机制

区块链动态访问控制应满足以下要求：

——节点权限应支持区块生成、区块同步、区块验证与广播以及发送交易；
——智能合约访问权限应支持接口访问控制、用户访问控制和混合访问控制；
——用户权限应支持注册用户权限和未注册用户权限，根据角色来区分注册用户权限；
——全局权限应支持用户部署和读取智能合约权限。

8.4 跨链机制

8.4.1 跨链交互要点

跨链交互应满足以下要点：
——宜支持通过如跨链可信通道类的跨链组件，将不同区块链网络打通，形成协同跨链网络；
——对于跨链可信通道类的跨链组件，宜支持将区块链传来的消息转换为CCIP结构的消息，也可以将CCIP结构的消息转换为特定区块链可以识别的交易格式；
——宜支持在跨链可信通道内借助跨链适配器类插件实现不同区块链的访问及智能合约的调用，并支持对交易指令及交易结果的验证；
——由省本级、地市州及部门级基础设施协同链网形成的统一协作链作为跨链体系的核心，应统筹管理跨链事务；
——应支持对区块链之间的跨链交互操作进行类型划分，规范跨链调用行为。

8.4.2 跨链交互协议数据结构

跨链交互协议数据见表10。

表10 跨链交互协议数据

数据元素	说明	是否必选
InID	跨链交互ID	必选
From	来源跨链服务，格式：<OrgID>:<BuChainID>:<Service ID>	非必选
To	目标跨链服务，格式：<OrgID>:<BuChainID>:<Service ID>	必选
Type	跨链交互类型，如跨链读数据、跨链写数据等	必选
InContent	跨链交互内容	必选
Timestamp	时间戳	必选
Proof	跨链交互证明	必选
Extend	扩展字段	非必选
Signature	跨链可信通道签名	非必选
Version	跨链协议版本号	非必选

9 区块链分布式应用层基本要求

9.1 业务与合约

9.1.1 合约机制的要素和标准流程

9.1.1.1 合约机制要素

合约机制要素应包括：

——自治：合约一旦启动就会自动运行，不需要其他干预；

——自足：合约能够通过提供服务或发行资产的自足方式，进行资源的获取和使用；

——去中心化：合约机制不依赖单个中心化服务器，通过网络节点实现分布式的自动运行。

9.1.1.2 合约机制标准流程

合约机制标准流程应包括：

a) 合约创建
- 两个及两个以上的用户注册为合约参与者；
- 参与者共同商定承诺，承诺包含了各方的权利和义务；
- 编写合约代码。

b) 合约部署
- 合约通过P2P方式在区块链网中扩散；
- 区块链网中的验证节点存储合约；
- 根据共识机制，验证节点将合约集合生成新的区块，扩散到全网验证。

c) 合约执行
- 定期遍历每个合约的状态机、事务以及触发条件；
- 基于事件触发，将满足触发条件的合约推送到验证队列；
- 事务验证；
- 达成共识，事务成功执行。

d) 合约完成
- 判断合约状态；
- 当合约包含的所有事务顺序执行完成后，状态机标记状态为“完成”；
- 从最新的区块中移除合约。

9.1.2 智能合约技术要求

9.1.2.1 去中心化自治组织

去中心化自治组织是区块链智能合约运行要件。

9.1.2.2 隐私保护

智能合约I/O应该具备隐私保护能力，应具备隐私保护能力，可以使用如同态加密，零知识证明等技术。

9.1.2.3 透明度

智能合约有权访问其部署到的区块链的人都可以读取和使用。智能合约的执行结果是可以被验证的。

9.1.2.4 时间效率

智能合约的执行具有即时性，一旦被调用或满足执行条件，即可立即执行，不需要任何时间来验证和处理信息并解决交易。

9.1.2.5 操作精度

智能合约的执行结果要保证都是精确的，完全没有人为错误。

9.1.2.6 可信性

智能合约在任何情况下都不会在执行协议时表现出偏见或主观性。

智能合约语言应具有非常高的成熟度，具有精确语法和语义的形式化语言来刻画系统的性质和行为，合约的生成和执行有标准的规范性约束。

9.2 服务与访问

9.2.1 区块链应用接口调用基本要求

区块链应用接口调用基本要求应包括：

——区块链应用中应确认 API 接口的权限控制，防止非授权调用；

——区块链应用中接口调用方式应支持 SDK，或者远程过程调用（RPC、RESTful）；

——区块链应用中应提供以下与区块相关的业务：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；

——区块链应用中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。

9.2.2 区块链应用接口调用方法

开发和调用区块链应用接口的调用方法如下：

——基于公有链已有协议和开源工具库等，开发或调用链上已有代码、协议和接口，实现区块链行业应用的目标功能；

——基于共链协议与开源工具库等，开发或调用链上代码和接口，搭建应用区块链底层，实现区块链行业应用的目标功能，基于共链的跨链技术，实现链与链之间的通信和价值交换；

——基于联盟链已有协议和工具库等，开发和调用链上代码和接口，实现区块链行业应用的目标功能；

——基于私有链已有协议和工具库等，开发和调用链上代码和接口，实现区块链行业应用的目标功能。

9.3 应用与监管

应用与安全风险监管要求包括：建立链上信息安全审核机制、建立链上信息安全监测预警机制、建立安全应急处理机制和建立负面清单机制。

——建立链上信息安全审核机制应包括：

- 建立区块链链上信息安全审核机制，采取包括人工审核、平台自动审核等技术手段，有效识别并及时停止发布违法信息、不良信息；
- 留存违法信息、不良信息的审核日志信息；
- 对审核发现的链上违法信息、不良信息，能够追溯到信息发送节点。

——建立链上信息安全监测预警机制应包括：

- 建立主动巡查监测机制，及时发现已经存在于区块链上的违法信息、不良信息；
- 对链上节点运行状态和信息发布状态进行监控，如发现运行异常节点及时排查预警；
- 建立信息安全预警机制，能够对存在安全风险的信息内容提前预警并及时核查处置；

- 建立投诉举报渠道，包括有效的电话、电子邮箱、网页反馈入口等，及时接受投诉举报并予以处理。

——建立安全应急处理机制应包括：

- 制定区块链信息溯源规则，提供交易信息溯源的相关技术措施，溯源信息的留存时间应不少于6个月；
- 制定节点异常应急处置措施，在区块链节点发生异常时，及时预警并切换灾备节点；
- 制定共识机制应急处置措施，在区块链节点数不足以支持当前共识机制时，及时预警并处置；
- 制定安全事件分级响应处置预案，定期开展安全事件应急演练；
- 根据实际情况对安全事件分级预案进行修订更新和版本控制。

——建立负面清单机制应包括：

- 建立区块链应用安全负面清单；
- 建立违法信息、不良信息数据库和异常行为用户列表，并定期维护更新。

10 区块链应用安全保障体系要求

10.1 总体安全

针对区块链应用面临的安全风险，应制定相应的技术安全要求，主要分为四个部分：基础设施层安全、基础资源层安全、应用支撑层安全和分布式应用层安全。

10.2 基础设施层安全

10.2.1 存储资源安全要求

区块链存储资源安全要求应包括：

——数据存储服务应保证账本数据的冗余性，防止因单个节点失效而造成总账本数据的丢失；

——数据存储服务应保证存储空间可扩展，满足高可用性。保证数据查询和更新等操作的响应时间，满足上层协议和应用的要求。

10.2.2 计算资源安全要求

区块链计算资源安全要求应包括：

——专用硬件与主机或其它节点通信时，建立安全的通信通道，敏感数据传输时以密文形式传输；

——专用硬件如需使用外部存储器件存储敏感数据，应对数据进行保护，以防止数据被恶意篡改或信息泄漏；

——专用硬件写出的数据如以密文的形式传输并存储于外部存储器，需采用完整性校验等方式，保护数据完整性；

——处理敏感信息的专用硬件应防止攻击者偷取保密信息。

10.2.3 网络资源安全要求

区块链网络资源安全要求应包括：

——同一个主机或机房不能创建超过特定数量的节点，避免单点风险；同时应提供白名单或者 PKI 证书机制进行节点准入限制；

——通过节点身份认证、分层网络路由以及限制来源 IP 数量等技术手段，应对常见的网络攻击；

——节点离线后重新加入系统的节点，应进行状态同步，保障账本的一致性；

——可动态配置节点通信的组网方式，单一节点故障不应影响节点的整网通信；
——对于支持共识节点动态加入或者删除的区块链，在节点加入或删除后共识协议仍保持一致性、活性和可用性，退出的节点个数不应超出阈值；
——节点通信应采用密码技术保障敏感信息传输的保密性和完整性；
——应对区块链网络状态进行全方位监控，监控指标包括但不限于在线节点个数、节点在线时长、区块同步时长、总交易数、总区块数、单个区块的交易数、平均出块时长、热点合约、合约个数、吞吐量（峰值）和交易延迟等。

10.3 基础资源层安全

10.3.1 链管平台能力及安全要求

10.3.1.1 链管平台应具备的区块链管理要求应包括：
——跨链链管宜采用 DID 标识符等方式作为参与链管的区块链设置唯一的身份标识；
——跨链链管宜支持对区块链的基础信息查看，如区块链名称、归属机构、共识方式等信息；
——跨链链管宜支持对区块链网络节点的信息查看，如节点名称、节点类型、运行状态等信息；
——跨链链管宜支持对区块链区块高度、交易总量等的信息查看。

10.3.1.2 链管平台安全要求应包括：
——应只允许通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计；
——应对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等；
——应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控；
——应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理；
——应对网络链路和服务器等的运行状况进行集中监测。

10.3.2 分布式数字身份平台安全要求

分布式数字身份平台安全要求应包括：
——身份认证接口应使用密码技术保证数据传输的完整性、保密性和不可否认性，同时应对敏感数据设计额外的保护机制；
——身份管理应实现对节点的准入和退出管理；通过对网络中节点进行安全性认证，实现过滤非法用户、过滤恶意节点、阻挡攻击者等功能；
——身份认证服务应通过密码技术保护用户隐私，采用双因素或多因素结合的身份认证技术。对于强身份认证场景使用数字证书等密码技术保证用户身份真实性。

10.3.3 数据管理平台安全要求

数据管理平台安全要求应包括：
——应采用校验技术或密码技术保证数据在传输过程中的完整性，包括但不限于鉴别数据、业务数据、审计数据、配置数据、视频数据和个人信息等；
——应采用密码技术保证数据在存储过程中的保密性，包括但不限于鉴别数据、业务数据和个人信息等；
——应提供数据的本地数据备份与恢复功能；
——应提供异地实时备份功能，利用通信网络将数据实时备份至备份场地。

10.4 应用支撑层安全

10.4.1 共识机制安全要求

共识机制安全要求主要包括：

——使用基于真实共识算法的共识机制，保持所有正确共识节点对区块链中从第一个区块到已确认的最后一个区块的一致性且不被更改；

——共识协议应具备一定的容错性，当恶意节点数小于阈值，协议仍可以正常运行；

——共识协议算法切换后，仍可满足一致性、活性、可用性，保障系统服务的完整性和连续性；

——共识节点从异常场景恢复后应能保证数据正常恢复、数据不丢失、正常参与共识流程；

——应定期对共识机制的安全性进行查验，保证共识机制安全有效地进行；

——应对加入共识机制的节点信息进行记录和身份验证，确保节点可追溯。

10.4.2 组网机制安全要求

组网机制安全要求应包括：

——应保证网络设备的业务处理能力满足业务高峰期需要；

——应保证网络各个部分的带宽满足业务高峰期需要；

——应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址；

——应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段；

——应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。

10.4.3 动态访问机制安全要求

动态访问机制安全要求应包括：

——应在网络边界或区域之间，根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信；

——应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化；

——应对源地址、目的地址、源端口、目的端口和协议等进行检查，控制数据包进出；

——应能根据会话状态信息为进出数据流提供明确的控制访问能力；

——应对进出网络的数据流实现基于应用协议和应用内容的访问控制。

10.4.4 跨链机制安全要求

跨链机制安全要求应包括：

——跨链应具有拜占庭容错性；

——一个区块链应能够接收和验证另一个区块链的数据；区块链不能否认自己发送信息的行为和内容，区块链确保验证过程正确执行，不可被篡改；

——对于支持资产或信息跨链的系统，由一个区块链发起的以变更双方状态为目的的跨链请求，应满足或者在源链和目标链都执行成功，或者在两个链都执行失败；

——应具备跨链事务仲裁机制接口；

——跨链消息中的隐私数据应事先得到相应区块链的授权；敏感的跨链数据应只被接收方获取，其他区块链或者链外服务不能获取；

——保证跨链的交易不应被恶意重播，不存在双重支付问题。

10.5 分布式应用层安全

10.5.1 业务与合约安全要求

智能合约安全要求主要包括：

——应在业务范围内提供符合其业务逻辑的智能合约；

——提供智能合约的生命周期管理，包括智能合约的创建、编译、部署、调用、冻结、解冻、升级和销毁等；

——应对智能合约的安全性进行审核，并保留审核记录；利用包括但不限于规则验证、静态分析、模糊测试和形式化验证等技术，在智能合约需求分析、设计、实现、测试和使用过程中进行安全审计，保证业务逻辑安全，源代码安全，二进制代码安全以及执行环境的安全，并保证智能合约的安全运行；

——应对智能合约的正确性进行审核，并保留审核记录；只有授权的合约可被部署，特定的合约只有特定的用户才可调用；

——应确保智能合约的可隔离性；除相互调用等方式外，一个智能合约不应修改其它智能合约的状态；智能合约与外部数据交互时，外部数据应只影响本智能合约的状态；

——确保智能合约的可结束性；智能合约应在有限时间内结束执行，不应出现无限循环等行为，防止长时间占用资源；

——在智能合约进行部署、调用、冻结、解冻、升级和销毁等操作时应要求用户通过电子签名等方式对相关操作进行权限验证授权。

10.5.2 服务与访问安全要求

服务与访问安全要求应包括：

——区块链业务提供者应提供区块链业务对外开放 API 接口，确保终端用户与区块链业务之间的安全通信；防止数据被恶意篡改攻击，保证重要数据以有效手段进行加密传输并进行完整性保护；防止中间人攻击，通信过程进行证书真实性、有效性检验；

——区块链业务提供者应制定权限管理机制，确保不同的用户只能访问和操作相对应的资源；

——区块链业务提供者应对账户对应用层的读写权限做好分级。