

ICS 35.240

CCS L 70

DB 31

上海市地方标准

DB 31/T 1460—2023

区块链跨链通用要求

Cross-chain general requirements of blockchain

2023-12-27 发布

2024-04-01 实施

上海市市场监督管理局 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

4 区块链跨链基本要求 2

5 区块链跨链参考架构 2

6 区块链跨链数据及接口要求 3

 6.1 跨链数据包的组成规范 3

 6.2 跨链服务接口 4

7 区块链跨链应用要求 5

8 区块链跨链安全要求 5

 8.1 安全基本要求 5

 8.2 数据安全 5

 8.3 接口安全 5

 8.4 接入安全 6

 8.5 权限控制 6

 8.6 运行安全 6

参考文献 7

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这些专利的责任。

本文件由上海市经济和信息化委员会提出并组织实施。

本文件由上海市信息标准化技术委员会归口。

本文件起草单位：上海计算机软件技术开发中心、上海浦江数链数字科技有限公司、上海软中智链数字科技有限公司、同济大学、蚂蚁区块链科技（上海）有限公司、上海玳鸽信息技术有限公司、复旦大学、上海市数字证书认证中心有限公司、上海万向区块链股份公司、上海信医科技有限公司。

本文件主要起草人：戴炳荣、王洒洒、李超、王虎、旷志光、陆明、朱雪雅、马小峰、周斌、张晓蒙、方玉书、丁凤、吕智慧、王鹏理、杜宇、李峻桦。

区块链跨链通用要求

1 范围

本文件规定了区块链跨链的基本要求、参考框架、数据及接口要求、应用要求和安全要求。
本文件适用于上海地区开展区块链跨链互操作的组织。

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—2018 信息安全技术 网络安全等级保护基本要求
- GB/T 42570—2023 信息安全技术 区块链技术安全框架
- 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

GB/T 42752—2023界定的以及下列术语和定义适用于本文件。

3.1

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。

[来源：GB/T 42752—2023，3.12]

3.2

同构区块链 homogeneous blockchain

在底层架构、数据接口、接口协议、安全机制等一致的区块链。

3.3

异构区块链 heterogeneous blockchain

在底层架构、数据接口、接口协议、安全机制等组织形式和机制拥有较大差异的区块链。

3.4

跨链 cross-chain

实现不同区块链间数据交换或数字资产交换的互操作行为。

注：根据所跨越的区块链底层技术平台的不同可以分为同构区块链跨链和异构区块链跨链。

3.5

加密 encipherment encryption

对数据进行密码变换以产生密文的过程。

[来源：GB/T 25069—2022，3.278]

3.6

源链 source chain

在跨链协议中，主动发起跨链请求的一方。

[来源：GB/T 42570—2023，3.17]

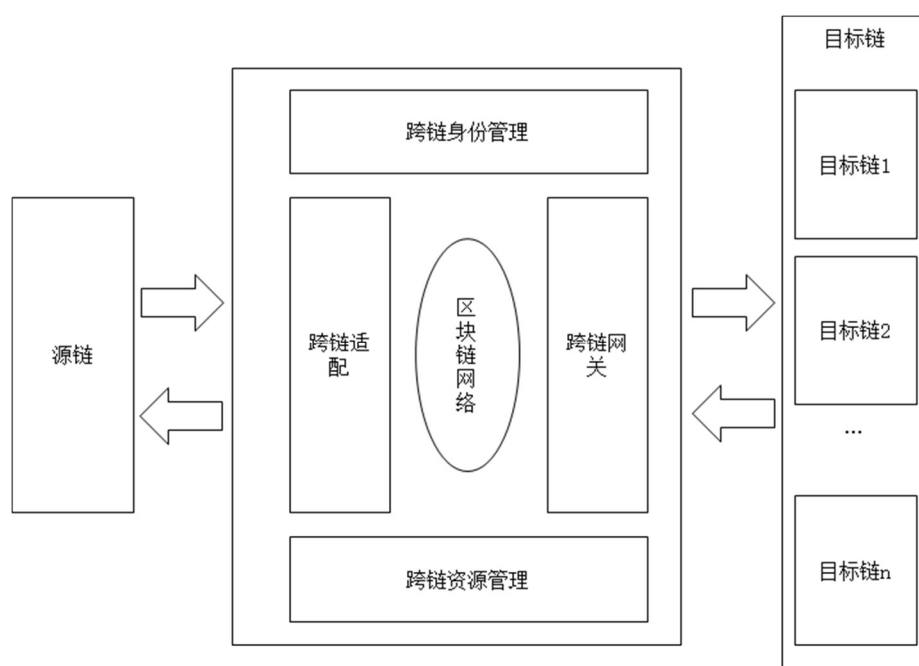


图1 区块链跨链参考架构

5.2 跨链身份管理旨在实现身份在多条链间的互通互认，应满足如下要求：

- a) 跨链身份标识应具有唯一性且全局可用；
- b) 区块链身份应由可信的身份签发者颁发；
- c) 支持区块链的身份管理，包括身份创建、授权等；
- d) 支持通过数字签名、多重签名等方法实现区块链跨链身份认证和权限管理；
- e) 支持跨链互操作参与者进行身份验证，并确保只有获得授权的参与者才能进行跨链交易操作。

5.3 跨链网关旨在实现跨链交易的传递，应满足如下要求：

- a) 支持建立安全加密的网络信道链接;
- b) 支持异构/同构区块链间数据交换;
- c) 支持失败重连。

5.4 跨链适配旨在实现同构/异构区块链间的跨链事务执行，应满足如下要求：

- a) 支持同构/异构链间互操作；
- b) 支持链上合约和链下插件两部分的适配。

5.5 跨链资源管理模块应满足如下要求:

- a) 具备同构/异构链的信道资源管理功能;
- b) 具备同构/异构链的合约资源管理功能;
- c) 具备同构/异构链的共识资源管理功能。

6 区块链跨链数据及接口要求

6.1 跨链数据包的组成规范

区块链跨链事务包括请求、操作、执行、提交等流程,事务执行成功则进行跨链事务提交,执行失败的跨链事务应有回滚机制,执行跨链事务回滚操作。跨链数据包的组成相关信息见表1。

表1 跨链数据包的数据组成

跨链事务类型	数据项	数据项要求
跨链事务请求	跨链事务的标识	●
	跨链源链的标识	●
	跨链目标链的标识	●
	跨链事务的合约名称	●
	跨链事务的合约调用方法	●
	跨链事务时间戳	●
	跨链事务内容信息	○
跨链事务操作	跨链事务的标识	●
	跨链源链的标识	●
	跨链目标链的标识	●
	跨链事务时间戳	●
	跨链事务操作的类型	○
	跨链事务内容信息	○
事务执行结果	跨链事务的标识	●
	跨链源链的标识	●
	跨链目标链的标识	●
	跨链事务执行结果	●
	跨链事务时间戳	●
	跨链事务操作的类型	○
跨链事务提交	跨链事务的标识	●
	跨链源链的标识	●
	跨链目标链的标识	●
	跨链事务操作的类型	○
	跨链执行结果	○
跨链事务回滚	跨链事务的标识	●
	跨链源链的标识	●
	跨链目标链的标识	●
	跨链事务操作的类型	○
	跨链执行结果	○
注：●为必选；○为可选。		

6.2 跨链服务接口

6.2.1 事件接口

事件接口主要是指事件监听，是上层应用对所关注业务实现自动化监听的关键技术，接口应包含订阅事件、取消订阅。

6.2.2 合约接口

智能合约是区块链和上层应用之间的业务层抽象，是链系统支撑复杂业务的关键支撑技术，智能合约接口应包含部署合约、启动合约、升级合约、停止合约、查询合约等。

6.2.3 交易接口

交易是区块链账本中基本数据单位，交易接口是应用开发者使用频次较高的接口类型，交易接口应包含交易组装、交易发送、交易校验、交易查询等。

6.2.4 区块接口

区块是区块链系统的关键数据结构，区块接口应包含区块签名、区块打包、区块收发、区块校验、区块查询等接口。

7 区块链跨链应用要求

7.1 区块链跨链应用应满足以下要求：

- a) 松耦合：跨链通道或锚定节点故障时，不应影响区块链的正常运行；
- b) 可信：跨链互操作过程应可追溯，跨链执行结果应可信；
- c) 安全可靠：跨链应用运行时，应满足信息的完整性、数据的隐私性和应用的可靠性。

7.2 区块链跨链应用运行流程宜包含以下步骤：

- a) 跨链应用部署：跨链应用部署指部署跨链事务、跨链合约等相关应用的过程；
- b) 跨链应用触发：跨链应用触发是指跨链服务使用方在使用跨链服务时发起跨链调用的过程；
- c) 跨链应用执行：跨链应用执行是指执行跨链调用和操作的过程；
- d) 跨链应用维护：跨链应用维护是指维护已部署跨链应用的过程；
- e) 跨链应用废止：跨链应用废止是指废弃已部署跨链应用的过程。

8 区块链跨链安全要求

8.1 安全基本要求

区块链跨链安全应满足以下基本要求：

- a) 符合 GB/T 42570—2023 中第 7 章的要求；
- b) 符合 GB/T 22239—2019 中 8.1.2 的要求。

8.2 数据安全

跨链数据安全应满足如下要求：

- a) 具备跨链交易端到端的完整性保护，使用安全加密算法对交易信息和资产进行加密保护；
- b) 具备跨链交易在源链和目标链之间的数据验证机制；
- c) 具备跨链通信端到端的信息加密保护；
- d) 提供数据变换技术，对敏感信息进行脱敏处理。

8.3 接口安全

跨链接口安全应满足如下要求：

- a) 支持接口访问调用频度设置和事务操作及账本查询缓存设置；
- b) 接口的访问权限等级分为低等级权限、中等级权限和高等级权限三类，针对不同的用户可以配置不同的访问权限；
- c) 满足可信计算环境的运行配置要求，支持跨链治理。

8.4 接入安全

跨链接入安全应满足如下要求：

- a) 支持身份验证功能，支持通过用户数字证书进行身份认证；
- b) 支持超时断开机制，验证超时后应断开用户会话或重新鉴别；
- c) 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。

8.5 权限控制

跨链权限控制应满足如下要求：

- a) 支持交易权限设置，实现读写权限分离，账本访问和链码访问权限分离；
- b) 支持分权分域，根据用户角色设置管理权限，对用户授权遵循最小权限原则；
- c) 提供跨链节点准入准出配置和节点事务处理及账本查询授权配置；
- d) 支持对跨链交易相关方进行身份认证。

8.6 运行安全

跨链运行安全满足如下要求：

- a) 应具备源代码安全审计服务，支持对跨链服务代码进行测试分析；
- b) 应支持部署及运维工具对跨链服务进行分析；
- c) 跨链应用服务提供方应具备应急响应机制和应急预案；
- d) 宜建立数据审核机制，保障跨链事务数据合规。

参 考 文 献

- [1] GB/T 5271.18—2008 信息技术 词汇
 - [2] GB/T 11457—2006 信息技术 软件工程术语
 - [3] GB/T 25069—2022 信息安全技术 术语
 - [4] GB/T 32399—2015 信息技术 云计算 参考架构
 - [5] DB31/T 1331—2021 区块链安全技术通用要求
-