ICS 35.020
CCS L 70

团　体　标　准

T/CESA XXXX—202X

区块链 开放联盟链接入技术要求

Blockchain—Access technical requirements for open consortium blockchain

征求意见稿

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

已授权的专利证明材料为专利证书复印件或扉页，已公开但尚未授权的专利申请证明材料为专利公开通知书复印件或扉页，未公开的专利申请的证明材料为专利申请号和申请日期。

202X-XX- XX 发布　　202X-XX- XX 实施

中国电子工业标准化技术协会　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。

本文件由中移动信息技术有限公司提出。

本文件由中国电子工业标准化技术协会归口。

本文件起草单位：

本文件主要起草人：

区块链 开放联盟链接入技术要求

1 范围

本文件规定了开放联盟链接入技术要求，包括基础管理要求、应用接入要求、跨链机制要求等方面。

本文件适用于指导开放联盟链的架构设计与研发使用。

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 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

GB/T 43572-2023 区块链和分布式记账技术 术语

3 术语和定义

GB/T 42570—2023、GB/T 42752—2023、GB/T 43572-2023中所规定术语以及下列术语和定义适用于本文件。

3.1 开放联盟链 open permissioned blockchain

对主流区块链框架通过技术改造而成，具备可扩展、可管理、数据开放等特性的区块链框架。

3.2 交易 transaction

区块链中的一种操作（例如，部署、调用和查询区块链合约），授权用户执行交易操作（例如，读取/写入区块链数据、调用区块链合约）。

3.3 区块链平台 blockchain platform

基于区块链相关技术建立的平台(或系统)。

注:区块链相关技术主要包括点对点通信、去中心化数据存储、群体共识机制和交易处理方法、权限管理等。

3.4 区块链数据 blockchain transaction

区块链中的数据，例如分布式账本信息、世界状态信息、权限策略等。

3.5 共识节点 consensus node

参与区块链网络中共识投票、交易执行、区块验证和记账的节点。

3.6 同步节点 sync node

参与区块和交易同步、区块验证，交易执行，并记录完整账本数据，但不参与共识投票的节点。

3.7 轻节点 light node

参与同步和校验区块头信息、验证交易存在性。

3.8 SPV 节点

不需要下载全部区块的数据，只需要下载全部的区块头数据，就可以验证支付的节点。

3.9 身份 identity

身份是指涉及自然人及法人等实体的属性的集合。在开放联盟链标准下，身份可以进行数字化标识，通过ID形式与链账户关联。

3.10 跨链 cross chain

实现在不同区块链之间的双向信息交互、信息验证与服务调用的互操作技术。

4 缩略语

下列缩略语适用于本标准。

SPV Simplified Payment Verification 简单支付验证

5 开放联盟链参考架构

开放联盟链是基于主流开源区块链底层框架，通过技术改造而成，具备可扩展、可管理、数据开放等特性，参考架构见图 1。

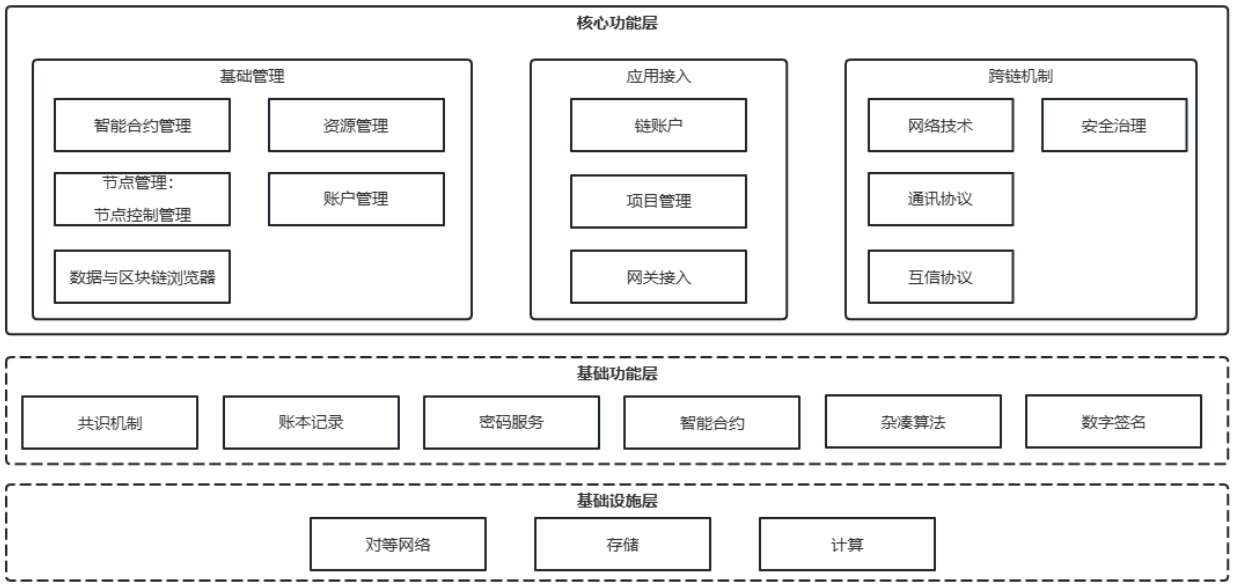

图 1. 开放联盟链参考架构

其中，基础设施层、基础功能层为区块链基础能力，符合 GB/T 42752-2023 相关规定。

核心功能层为开放联盟链区别于常规区块链的重要因素，包括基础管理、应用接入、跨链机制等方面。

基础管理主要用于智能合约、资源、节点、账户、数据等管理；应用接入包含链账户、项目管理以及网关接入；跨链机制包含网络技术、通讯协议、互信协议和安全治理部分。

6 基础管理要求

6.1 智能合约控制管理

6.1.1 功能要求

智能合约应具备可编程性，合约代码在运行期间应能获得一些必须的链上数据支持。

a）合约代码在运行时应能获得当前区块的相关数据（区块高度等）；

b）合约代码在运行时应能获得当前交易的相关数据（交易发起方、交易输入参数等）；

c）合约代码在运行时应能获取相关的链上状态数据（当前余额等），在合约设定的验证条件（签名或hash等）满足时，应能修改相关的链上状态；

d）合约代码在运行时可以根据设计准许或拒绝某个操作；

e）宜支持智能合约IED。

6.1.2 合约治理

应符合如下要求：

a) 合约拥有者可进行合约部署、升级、调用；

b）合约管理者可对合约进行冻结、解冻等操作。

6.2 节点控制管理

开放联盟链节点可区分，根据节点是否参与共识、是否验证区块、是否执行交易等区分节点类型。应包含如下类型节点：

a）共识节点

b）同步节点

同时根据实际应用场景宜包含如下类型节点：

a）SPV节点

b）轻节点

6.2.1 节点接入

开放联盟链应为用户提供通过自建节点的方式加入开放联盟链网络的能力，节点接入应符合以下要求

a）节点接入申请，开放联盟链应当拥有提供外部节点提交加入申请的完整功能，可以通过接口、平台或者链自身等机制实现；

b）节点信息核查，开放联盟链运营方应当对申请加入网络的外部节点提交的信息进行身份合规审查；

c）节点准入，联盟为通过审查的外部节点颁发开放联盟链网络准入凭证；

d）节点验证，当用户自建节点接入开放联盟链网络时，链节点应当可以通过自身链的机制或者其他组件对加入网络的节点凭证进行验证；

e）支持节点白名单机制。

6.2.2 节点退出

开放联盟链应当有完整的节点退出机制，当节点退出网络时，链的其他的节点可以实时的对正在连接的链节点进行中断，阻止已经退出的节点继续接入网络。

6.2.3 节点健康检查

需支持节点健康检查与预警通知。

6.3 算力资源管理

对于账户执行合约、其他交易的操作，应提供一种指标，对操作的计算资源进行计数或者进行转换的机制，在该机制中所使用的用于表示剩余使用资源的指标，应禁止它们在普通的账户之间进行转移。

6.4 账户管理

6.4.1 身份管理要求

a）身份注册需通过身份注册机构完成身份实名注册并对身份进行核实，在完成身份注册与核实后应生成全局唯一身份标识 ID；

b）身份鉴别应提供专门的组件或模块实现用户身份实名认证功能，该组件或模块应确保正确标识和鉴别相关身份实体信息和授权信息。

6.4.2 链账户基本要求

a）链账户应与其所在的区块链上的各类数字资产或智能合约关联绑定；

b）每个链账户应在创建时即关联一个身份标识ID，链账户与身份标识ID应支持多对一和一对一关联。

6.4.3 链账户治理要求

对身份实体的隐私保护行为应至少满足GB/T 35273-2020中的“个人信息安全基本原则”。除此之外，应符合以下要求：

a）在收集具体数据信息或生物识别信息前需告知身份实体对象收集的具体用途；

b）收集身份实体对象的数据信息或生物识别信息需确保最小必要原则且需获得身份实体授权同意；

c）所有收集的敏感信息涉及存储和传输的，均需采用加密处理等安全措施，且存储周期需告知身份实体；

d）保证链账户的私密性和安全性，技术上不得留存或窥视链账户的密钥信息；

e）提供链账户的基本操作：

开通：指在链上生成一个新的链账户；
注销：指链账户不可使用，但在链上保留链账户过往的所有信息；
冻结：指限制账户的活动，不允许链账户进行任何功能操作；
解冻：指恢复链账户的活动，允许链账户进行正常的功能操作。

6.4.4 用户审查要求

应通过关联链账户(包括公私钥)与实名身份实体，保证开放联盟链体系下所有区块链平台链账户能追溯到具体身份实体, 并能明确具体身份实体在具体应用场景下涉及的具体链账户的交易数据及所属的数字资产。

6.5 区块链浏览器

宜支持区块链浏览器，区块链浏览器应具备以下功能：

a) 区块和交易浏览：区块链浏览器应允许用户轻松地查看区块链网络上的所有区块和交易。每个区块包含一系列交易记录，而每笔交易则包含有关智能合约执行的详细信息。用户可以浏览每个区块中的交易，以及区块之间的链接关系。
b) 检测链上信息的用户概况：区块链浏览器应提供了及时、便捷的链上信息入口，帮助用户快速、准确地获取所需要的信息，包括相应地址的资产数量、交易区块信息等。
c) 地址查询：区块链浏览器应支持用户通过输入地址来查询特定的账户或钱包，并查看相关的交易历史和余额等信息。
d) 追溯数据信息：所有数据和信息都会在链上留下不可篡改前后接续的记录，通过区块链浏览器，用户应可以清晰地看到客观的链上交易路径。
e) 搜索功能：可以输入区块链的哈希值、区块高度或者具体某一笔交易的哈希值进行精准查询，区块链浏览器应返回给你账本中对应的数据。
f) 多链支持：浏览器应支持多类型区块链，用户可以切换查看不同区块链的数据，方便跨链比较和分析。
g) 实时交易监控：应提供实时更新的交易列表，允许用户监控最新的交易活动，包括新的区块生成和交易确认。
h) 统计展示：区块链浏览器应向用户展示区块链运行的统计数据，包括网络运行时长、节点数量、平均出块时间、TPS、交易曲线等，这些统计信息都可以辅助用户了解区块链网络运行状态，健康状态，业务活跃度等。
i) 网络状态监控：用户可以通过区块链浏览器监控整个区块链网络的状态。这包括网络的哈希率、区块间隔、活跃节点数量等指标。

7 应用接入要求

应方便用户简单、快速地接入区块链网络，满足接入要求。

7.1 链账户管理

开放联盟链应具备离岸账户管理能力，且应符合以下要求：

a）链账户类型应支持主流密码算法类型，包括SM2、RSA、ECDSA等；
b）应允许用户自行创建、保管链账户信息（私钥、账户地址），并对上链进行离线签名。

7.2 项目管理

项目管理是对用户接入开放联盟链系统的访问权限的管理，提供项目管理能力应符合以下要求：

a）应提供完整的项目管理生命周期，包含创建、修改、删除等阶段；

b）宜提供按照项目的访问控制功能。

7.3 网关接入

网关接入是开放联盟链为无法直接通过节点接入的用户提供区块链接入能力的组件，应符合以下要求：

a）应在网关中提供访问控制功能；
b）应使用通讯加密技术保证网关访问数据的安全性；
c）应提供高可用网关保证用户访问的稳定性；
d）宜提供详细的网关接入文档和SDK提升用户接入的便捷性。

8 跨链机制要求

8.1 跨链网络技术要求

跨链网络宜由基于公证人（单签或多签）的跨链框架、基于中继链的跨链框架、基于哈希时间锁的跨链框架或其他跨链框架来构建。

8.2 跨链接入要求

a）宜采用审核登记方式对接入跨链网络的同构或异构底层链进行准入管理；

b）宜提供开放接口、SDK以及适配器等接入方式，实现不同底层链适配接入跨链网络。

8.3 跨链通讯协议技术要求

a）宜采用跨链通讯协议实现源链上的跨链消息路由到目标链；

b）宜对区块、交易等关键数据结构进行抽象，构建统一的跨链数据结构和跨链消息格式，实现跨链消息在源链和目标链上的互通互认。

8.4 跨链数据互信技术要求

a）宜提供跨链验证机制来验证跨链消息的有效性，提供一种可验证方式，维护源链信任和目标链信任；

b）跨链网络或目标链接收到跨链消息后宜验证跨链消息有效性；验证通过后才能执行相应的跨链操作；

c）必须保证跨链交易的最终性，跨链交易执行结束后不会被撤销或更改，执行成功的跨链交易不会被回滚，执行失败的跨链交易不会因为时间推移而成功；

d）必须保证跨链交易的原子性执行，若跨链交易包含多个子交易，当且仅当所有子交易执行成功后，整个跨链交易才会最终确认到联盟链中，若任何一个子交易执行失败，已经执行成功的子交易必须撤销，同时将链状态回滚至交易被触发之前的状态；

e）开放联盟链必须保证跨链交易的一致性，源链和目标链在跨链交易执行前后的链状态必须保持一致，若跨链交易执行成功，源链和目标链上新的链状态合法有效，如果跨链交易执行失败，源链和目标链的链状态必须回滚。

8.5 跨链安全治理技术要求

a）宜采用安全手段来管理跨链事务，如跨链权限控制和验证、跨链事务的链上留痕以及链下存档、跨链事务过程全透明、跨链事务可追溯可验证、非法跨链事务预警机制和回滚机制、建立审计监管节点对跨链事务进行安全审计等技术手段；

b）宜采用隔离手段确保跨链网络安全，实现网络里某一条链出现安全事件时能快速地从跨链网络里隔离出去；

c）宜采用节点证书等方式确保跨链参与方的身份安全、跨链参与方之间的互信以及跨链参与方发起跨链事务的合法性，实现安全的多方跨链共治；同时宜引入审计监管节点对节点证书进行合规审计；

d）宜采用最终一致性对账技术来确保源链和目标链在跨链前后链状态变更的一致性；

e）宜采用跨链通信安全机制、跨链合约审计、节点证书管理、密钥管理、跨链权限管理、安全沙盒、恶意节点惩处机制等技术手段来构建安全的跨链环境。

参 考 文 献

[1] GB/T 5271.18—2008 信息技术 词汇 第18部分：分布式数据处理
[2] GB/T 43575-2023 区块链和分布式记账技术 系统测试规范
[3] GB/T 43579-2023 区块链和分布式记账技术 智能合约生命周期管理技术规范
[4] T/CESA 1221—2022 区块链 专用服务网络 基础设施总体要求
[5] T/CESA 6001—2016 区块链 参考架构
[6] T/CESA 1262-2023 区块链 链间互操作指南