ICS 03.060
CCS A 11

Q/ZXJTIT

中信建投证券股份有限公司企业标准

Q/ZXJTIT 002—2025

证券业跨链技术标准

Cross-Chain Technology Standard for the Securities Industry

2026 - 03 - 03 发布　　2026 - 03 - 03 实施

中信建投证券股份有限公司 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。

本文件由中信建投证券股份有限公司提出。

本文件由中信建投证券股份有限公司归口。

本文件起草单位：中信建投证券股份有限公司、中信建投基金管理有限公司、上证所信息网络有限公司、北京大学。

本文件主要起草人：张强、陶剑峰、何建欣、任平、高聪伟、张欣宇、李伟平、蔡楚煌、张栋、张宇聪。

本文件及其所代替文件的历次版本发布情况为：

——2026 年首次发布；

——本次为首次发布。

引　言

1　背景与意义

随着证券市场数字化转型加速，异构区块链系统间的协同需求日益迫切。当前券商交易链、登记结算链、监管链等多链并存，形成"数据孤岛"，导致跨机构业务流程效率低下。目前，跨链业务处理延迟较单链业务高出数倍。本标准通过建立统一跨链技术体系可以提高交易结算效率，降低跨链数据验证成本，同时提高监管合规响应时间。

2　制定目的

旨在构建证券行业跨链技术的统一：
——统一跨链协议标准，解决异构链兼容性问题；
——统一数据交互规范，实现跨链数据语义一致；
——统一安全防护体系，保障跨链交易可信执行；
——统一监管对接接口，支持穿透式监管要求。

证券业跨链技术标准

1 范围

——业务场景：涵盖证券交易、登记结算、客户管理等各类核心和非核心业务；
——技术主体：

- 证券经营机构（券商/基金公司）自建区块链；
- 交易所主导的联盟链系统；
- 监管机构部署的监管链平台。

——地域范围：境内证券市场跨链业务（跨境场景需额外满足外汇管理要求）。

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。

SF/T 0076 电子数据存证技术规范[3]
JR/T 0314 区域性股权市场跨链技术规范[5]
ISO 20022 金融报文标准[8]

3 术语与定义

3.1 跨链互操作（Cross-Chain Interoperability）

指通过技术手段实现不同区块链系统间的数据交换与业务协同，包含：
——资产跨链：证券资产在不同链间的转移（如股票从交易链到清算链）；
——数据跨链：业务数据的跨链验证（如客户身份信息的跨链查询）；
——合约跨链：智能合约的跨链调用（如清算合约触发交易链结算）。

3.2 共识节点（Consensus Node）

参与区块链共识过程的核心节点：
——监管共识节点：由证监会部署，拥有数据优先验证权；
——券商共识节点：头部券商按区域部署，参与跨链共识；
——司法存证节点：连接法院司法链，负责证据固化。

3.3 监管链（Global Regulation Blockchain）

由中国证监会主导建设的联盟链，具备：
——全行业数据视图：聚合各业务链关键数据；
——监管规则引擎：内置反洗钱、适当性管理等合规规则；
——跨链监管接口：支持实时数据穿透式监管。

3.4 地方业务链（Regional Business Blockchain）

券商/交易所部署的业务专用链，如：
——交易链：处理证券委托交易，TPS≥5000；
——清算链：负责资金清算，支持 7×24 小时连续运行；

——客户链：管理客户身份与权限，符合 KYC/AML 要求。

3.5 **数据对象**（Data Object）

证券跨链业务中的核心数据实体：

```
class SecurityDataObject:
    def __init__(self, obj_type, data_id):
        self.obj_type = obj_type # 主体/账户/产品等类型
        self.data_id = data_id # 全局唯一标识符
        self.timestamp = get_utc_time() # 生成时间戳
        self.hash = calculate_hash() # 数据哈希值
```

3.6 **默克尔证明**（Merkle Proof）

用于验证跨链数据完整性的密码学结构：

——证明生成：将交易数据生成默克尔树，提供路径证明；

——验证效率：10 万笔交易的证明验证时间<50ms；

——存储优化：仅需存储树哈希值，节省 90%存储空间。

3.7 **智能合约**（Smart Contract）

跨链场景下的特殊要求：

——跨链调用：支持通过中继链触发跨链合约；

——共识验证：合约执行结果需经 3/4 以上共识节点确认；

——版本控制：支持合约灰度升级，确保跨链兼容性。

3.8 **安全沙箱**（Security Sandbox）

隔离运行跨链业务的安全环境：

——资源限制：单沙箱 CPU/内存资源上限控制；

——网络隔离：沙箱间通过防火墙隔离，仅开放必要端口；

——行为监控：实时监控沙箱内合约调用与数据访问。

3.9 **异常交易识别**（Anomaly Transaction Detection）

基于 AI 的跨链交易风控模型：

——特征维度：包含交易金额、频率、对手方等 20+维度；

——识别准确率：正常交易误报率<0.1%，异常交易召回率>95%；

——响应机制：发现异常时自动触发跨链交易冻结。

4 技术框架

4.1 协议层

4.1.1 跨链互操作协议（CCIP）

采用三层协议架构：

——传输层：基于 P2P 通信，支持节点自动发现与连接；

——信令层：定义跨链消息格式（请求/响应/事件）；

——业务层：封装证券特有的跨链业务流程（如转托管）。

4.1.2 路由协议（动态路径优化）

——路径计算：根据节点负载、网络延迟等 5 维指标动态计算最优路径；

——故障切换：主路径故障时，100ms 内切换至备用路径；
——流量均衡：按权重分配跨链流量，避免单点过载。

4.1.3 接口规范（RPC/TLS/HTTPS）

——RPC 接口：采用 JSON-RPC 2.0 标准，定义跨链操作接口；
——安全传输：TLS 1.3+国密套件（SM2+SM4）；
——接口限流：单节点每秒最多处理 500 次跨链请求。

4.1.4 中继链架构（Relay Chain Topology）

——核心中继链：由证监会、沪深交易所等 n 家机构节点组成；
——区域中继链：按华东/华北等区域部署，连接地方业务链；
——跨中继链：支持不同区域中继链间的通信，延迟<200ms。

4.2 数据层

4.2.1 数据模型（Data Model）

证券跨链核心数据模型，见图 1：

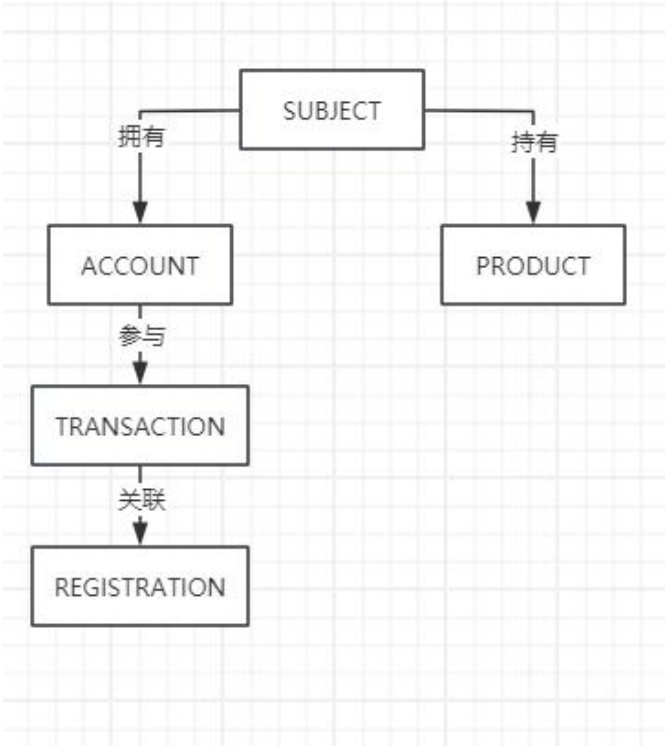

图 1　跨链核心数据模型

4.2.2 数据格式（JSON Schema）

跨链数据标准格式：

```
{
  "header": {
    "version": "1.0",
```

```
    "chainId": "0x001",
    "txId": "202507010001",
    "timestamp": "2025-07-01T09:30:00.000Z",
    "signature": "sig123456..."
  },
  "body": {
    "dataType": "SECURITY_TRANSFER",
    "sourceChain": "TRADING_CHAIN",
    "targetChain": "CLEARING_CHAIN",
    "data": { /* 业务数据 */ }
  }
}
```

4.2.3 数据生命周期管理

——创建阶段：跨链数据需经双链共识确认；
——更新阶段：仅允许追加记录，禁止直接修改；
——归档阶段：超过 1 年的非活跃数据归档至冷存储；
——删除阶段：按《证券法》要求保留至少 20 年。

4.3 安全层

4.3.1 加密算法（SM2/SM3/SM4）

——签名验签：SM2 算法，密钥长度 256 位；
——哈希计算：SM3 算法，生成 256 位哈希值；
——数据加密：SM4 算法，分组长度 128 位，CBC 模式。

4.3.2 身份认证（数字证书/多重签名）

——节点身份：使用国密 CA 颁发的 X.509 证书；
——交易签名：重要跨链交易需 3 家以上机构节点多重签名；
——权限控制：基于 ABAC 模型，支持 10 级权限粒度。

4.3.3 隐私保护（零知识证明/多方计算）

——监管查询：使用零知识证明向监管机构证明数据合规性，不泄露具体内容；
——跨链对账：采用多方计算技术，在不暴露原始数据的前提下完成对账；
——敏感字段：如账户余额，采用同态加密技术处理。

4.3.4 安全沙箱机制

——沙箱环境隔离：

```
sandbox:
  cpu: 4 cores
  memory: 8GB
  network:
    inbound_ports: [8080, 9090]
```

```
    outbound_ports: [443]
```

——异常交易识别模型：

- 规则引擎：内置 50+条证券行业特有风控规则；
- 响应策略：根据风险等级实施警告/冻结/拦截。

4.4 治理层

4.4.1 跨链治理结构

——监管链与业务链协同治理框架：

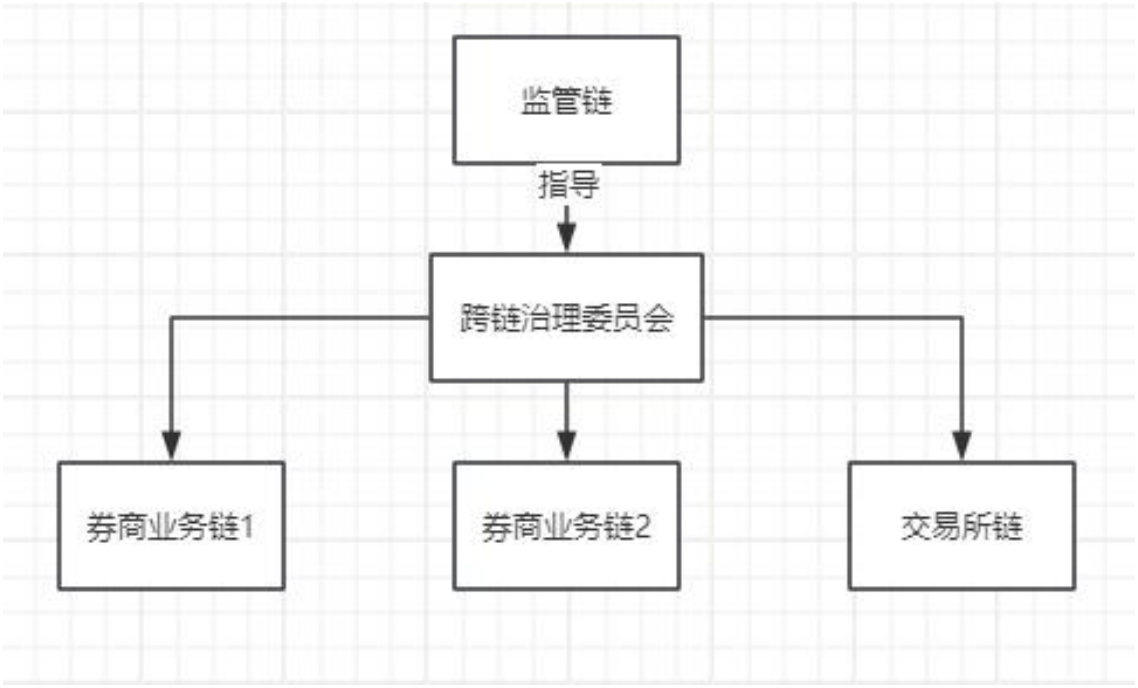

图 2　监管链与业务链协同治理框架

——多签投票机制：

- 普通提案：需 51%共识节点同意；
- 重大变更：需 75%共识节点同意（监管节点权重占 30%）。

4.4.2 数据治理规范

——跨链数据标准定义：

跨链数据标准定义

字段名称	类型	长度	约束条件
version	string	3	固定为 “1.0”
chainId	string	4	符合链标识编码规则（如 “0x001”）

txId	string	12	全局唯一交易 ID
timestamp	string	24	符合 ISO 8601 格式（如“2025-07-01T09:30:00.000Z”）
signature	string	-	符合国密 / SHA256 签名规则
dataType	string	20	固定枚举值（如“SECURITY_TRANSFER”）
sourceChain	string	20	固定枚举值（如“TRADING_CHAIN”）
targetChain	string	20	固定枚举值（如“CLEARING_CHAIN”）

——模板版本控制：

- 版本号规则：主版本.次版本.修订号（如 1.2.3）；
- 灰度发布：新模板先在 10%节点试点，72 小时后全量部署。

4.4.3 合规审查机制

——跨链事务预审：

- 反洗钱检查：交易对手方黑名单校验；
- 适当性管理：投资者风险等级与产品匹配度检查；
- 额度控制：单笔跨链交易金额不超过 500 万元。

——链上治理留痕：

- 提案记录：包含提案内容、提出者、时间戳；
- 投票记录：记录每个节点的投票结果与时间；
- 执行记录：治理决策的具体实施过程。

5 功能要求

5.1 互操作性

5.1.1 异构链接入

——公链兼容：支持以太坊、BSC 等主流公链接入；
——联盟链兼容：适配 FISCO BCOS、蚂蚁链、长安链等；
——接入流程：

- 链信息注册（链 ID/共识算法/接口地址）；
- 兼容性测试（100+标准测试用例）；
- 共识节点接入（至少 3 个跨链节点）。

5.1.2 数据同步与验证

——默克尔证明验证：

```
def verify_merkle_proof(transaction, proof, root_hash):
    current_hash = hash(transaction)
    for node in proof:
        current_hash = hash(current_hash + node) if is_left else hash(node + current_hash)
    return current_hash == root_hash
```

——状态根同步：

- 同步频率：每 10 个区块同步一次状态根；
- 验证时间：100 万条记录的状态根验证<1 秒；
- 差异处理：发现状态不一致时，触发全量数据同步。

5.2 安全性

5.2.1 交易防篡改

——哈希链机制：每个跨链交易包含前一笔交易的哈希值；
——数字签名：交易需经源链和目标链双签名确认；
——时间戳锚定：交易时间戳需经国家授时中心校准。

5.2.2 节点准入控制

——拜占庭容错：采用 PBFT 算法，容忍≤(n-1)/3 的恶意节点（n 为共识节点数）；
——节点白名单：新节点加入需经 2/3 以上现有节点投票通过；
——节点监控：实时监控节点在线率、共识参与度等 12 项指标。

5.2.3 智能合约审计

——漏洞扫描：使用 Slither 等工具进行静态分析；
——形式化验证：关键合约采用 TLA + 进行形式化验证；
——沙箱测试：新合约先在安全沙箱中运行 30 天，无异常后上链。

5.3 隐私保护

5.3.1 敏感数据脱敏

——脱敏规则：

脱敏规则

字段	脱敏方式	示例
身份证号	前 6 位+后 4 位，中间*	110101********1234
银行账号	前 4 位+后 4 位，中间*	6222****8888
交易金额	整数保留到万位，小数位保留后 2 位，中间*	123****.00

5.3.2 最小化信息披露

——业务场景与披露级别映射：

```
{
  "securities_transfer": {
    "required_info": ["securityCode", "quantity", "price"],
    "optional_info": ["clientId", "orderId"],
    "sensitive_info": ["clientBankAccount"]
  }
}
```

5.4 交互行为存证

5.4.1 全流程记录

——记录范围：

- 跨链请求发起：源链交易哈希；
- 中继处理：中继节点操作日志；
- 目标链执行：目标链交易哈希；
- 结果反馈：跨链结果状态码。

5.4.2 可追溯性

——时间戳精度：UTC 时间，精确到毫秒；
——行为链深度：至少保存 1000 条历史行为记录；
——追溯接口：支持按时间、交易 ID、参与方等维度查询。

5.4.3 合规性存证

——监管接口：

- 实时上报：重大交易事件发生后 10 秒内上报；
- 批量报送：每日凌晨 1 点前报送前一日全量数据。

——存证格式：符合 SF/T 0076-2020 电子数据存证规范[3]。

5.5 治理与合规

5.5.1 跨链数据模板管理

——模板生成：

- 协同定义：监管链与业务链共同制定模板；
- 自动化生成：根据数据模型自动生成 JSON Schema。

——权限控制：

- 模板查看：仅治理委员会成员可查看所有模板；
- 模板修改：需监管节点与 2/3 家以上券商节点同意。

5.5.2 治理事件响应

——争议仲裁流程：

- 争议提交：任何节点可提交争议申请；
- 证据收集：系统自动收集跨链相关证据；

- 仲裁投票：治理委员会成员进行投票；
- 结果执行：按仲裁结果执行相应操作。

——决策追踪：

- 决策记录：上链保存治理决策内容；
- 执行监控：实时监控决策执行进度；
- 效果评估：决策执行后 7 天内完成效果评估。

6 数据规范

6.1 数据分类与模型

6.1.1 主体对象（机构/个人/中介）

——核心字段：

- 主体 ID：全局唯一标识符，格式为"SEC-ENTITY-YYYYMMDD-NNNN"；
- 主体类型：枚举值（个人/法人/中介机构）；
- 身份信息：身份证号/统一社会信用代码（加密存储）。

6.1.2 账户对象（证券 / 资金 / 游客账户）

——账户类型：

- 证券账户：记录证券持有情况，关联股东代码；
- 资金账户：记录资金余额与流水，关联银行账户；
- 游客账户：临时账户，限制交易功能。

6.1.3 产品对象（股权/债券/基金）

——产品标识：

- 证券代码：如"600000.SH"（上海证券交易所代码）；
- 产品类型：股权/债券/基金/衍生品等；
- 发行信息：发行主体、发行规模、期限等。

6.1.4 登记对象（主体/账户/行为等）

——登记类型：

- 主体登记：记录主体基本信息与资质；
- 账户登记：账户开立、变更、注销记录；
- 行为登记：跨链交易、权限变更等行为记录。

6.2 数据存储要求

6.2.1 链上存证

——存证内容：

- 数据哈希值：采用 SHA-256 算法；
- 元数据：包含数据类型、时间戳、操作方等；
- 共识记录：参与共识的节点列表与签名。

——存储周期：永久保存。

6.2.2 链外存储

——存储架构：

- 对象存储：采用 AWS S3 兼容接口，支持海量非结构化数据存储；
- 数据库：使用分布式数据库，支持高并发查询。

——备份策略：

- 实时备份：关键数据变更实时备份；
- 异地容灾：数据同步至异地机房，RPO≤10 分钟。

6.2.3 跨链引用

——URI 标识：

- 格式：chain://{chainId}/{dataType}/{dataId}；
- 示例：chain://0x001/security/600000.SH。

——版本管理：

- 引用版本号：每次跨链引用需指定数据版本；
- 兼容性检查：引用时自动验证版本兼容性。

6.3 数据接口规范

6.3.1 区块链网络信息查询

——接口功能：

- 获取链基本信息：链 ID、共识算法、区块高度等；
- 查询节点状态：节点在线率、共识参与度等；
- 网络统计：近期跨链交易量、延迟等指标。

6.3.2 区块与交易信息获取

——区块查询：

- 按高度查询：获取指定高度的区块信息；
- 按时间查询：获取指定时间范围内的区块。

——交易查询：

- 按交易 ID 查询：获取交易详情；
- 按地址查询：获取指定地址的交易历史。

6.3.3 共识状态验证接口

——共识验证：

- 验证区块共识：检查区块是否经合法共识确认；
- 验证交易共识：检查交易是否被共识节点确认。

——状态证明：

- 生成默克尔证明：为指定数据生成证明；
- 验证证明：验证默克尔证明的有效性。

7 安全要求

7.1 密码算法合规性

7.1.1 国密算法强制应用

——必须使用的国密算法：

- SM2：用于数字签名和密钥交换；
- SM3：用于哈希计算和消息认证；
- SM4：用于数据加密和解密。

——算法实现要求：

- 符合 GM/T0004-2012《SM3 密码杂凑算法》；
- 符合 GM/T0003-2012《SM2 椭圆曲线公钥密码算法》；
- 符合 GM/T0002-2012《SM4 分组密码算法》。

7.1.2 证书格式

——数字证书标准：

- 符合 GB/T 20518-2018《信息安全技术 公钥基础设施 数字证书格式》；
- 采用 ASN.1 编码，遵循 X.509 v3 格式。

——证书内容要求：

- 主体信息：证书持有者的唯一标识；
- 公钥信息：与私钥对应的 SM2 公钥；
- 有效期：证书的有效时间范围；
- 发行者：颁发证书的 CA 机构。

7.2 业务数据安全

7.2.1 生成主体认证

——实名认证要求：

- 个人：身份证+人脸识别，符合央行 KYC 要求；
- 机构：营业执照+法人认证，通过工商系统核验。

——身份凭证：

- 生成主体唯一标识：基于 SM2 算法生成身份密钥对；
- 凭证有效期：定期更新（个人 1 年，机构 3 年）。

7.2.2 完整性保护

——数字摘要：

- 采用 SM3 算法计算数据摘要；
- 摘要值随数据一同存储和传输。

——消息认证码：

- 使用 HMAC-SM3 算法生成消息认证码；
- 用于验证数据在传输过程中的完整性。

7.2.3 传输加密

——传输协议：

- 采用 TLS 1.3 协议，启用国密套件；

- 加密套件组合：TLS-SM4-GCM-SM2-SM3。

——专线传输：

- 重要跨链数据通过金融专用网传输；
- 专线带宽：核心节点间专线带宽≥10Gbps。

7.3 链与节点安全

7.3.1 拜占庭容错共识

——共识算法：

- 采用 PBFT 或其变种算法；
- 共识节点数 n，可容忍 f≤(n-1)/3 个恶意节点。

——共识流程：

- 预准备阶段：主节点广播交易；
- 准备阶段：节点验证并广播准备消息；
- 提交阶段：节点验证并广播提交消息；
- 确认阶段：达到 2f+1 条提交消息后确认。

7.3.2 访问控制

——网络访问：

- IP 白名单：仅允许授权 IP 访问节点接口；
- 端口控制：只开放必要服务端口，关闭默认端口。

——API 访问：

- 令牌认证：使用 JWT 令牌，有效期 15 分钟；
- 权限分级：根据角色分配不同 API 访问权限。

7.3.3 恶意代码防范

——可信执行环境：

- 节点运行在可信执行环境（TEE）中；
- 使用 Intel SGX 或国产可信计算芯片。

——代码签名：

- 节点软件需经官方代码签名；
- 启动时验证代码完整性。

——实时监控：

- 部署入侵检测系统（IDS）；
- 实时扫描节点文件系统变化。

7.4 跨链应急安全机制

7.4.1 网络延时应急处理机制

——延时监测：

- 实时监测跨链网络延时，设置阈值（如 500ms）；
- 超过阈值时触发预警。

——应急措施：

- 切换备用网络路径；
- 降低跨链交易频率；
- 启动本地缓存机制。

7.4.2 应急响应方案

——响应流程：

- 事件检测：通过监控系统发现安全事件；
- 事件评估：判断事件严重程度和影响范围；
- 应急处置：启动相应级别的应急预案；
- 恢复重建：事件处置后恢复系统正常运行；
- 总结改进：分析事件原因，完善安全措施。

——预案类型：

- 节点故障：备用节点自动接管；
- 数据泄露：立即冻结相关数据，通知相关方；
- 共识异常：启动共识恢复流程，重新同步数据。

8 实施指南

8.1 部署与配置

8.1.1 硬件与网络要求

——核心节点硬件配置：

硬件配置

组件	配置要求
CPU	8 核以上，主频≥3.0GHz
内存	64GB 以上
存储	SSD 2TB 以上，RAID 10
网络	双万兆网卡，冗余连接

——网络架构：

- 内部网络：部署在金融专用网内；
- 外部网络：通过防火墙隔离，仅开放必要端口；
- 专线连接：核心节点间通过专线连接，延迟<5ms。

8.1.2 节点部署

——部署模式：

- 多中心化容灾：至少部署 3 个中心节点，分布在不同机房；
- 区域节点：按地域部署区域节点，覆盖全国主要城市。

——节点拓扑：

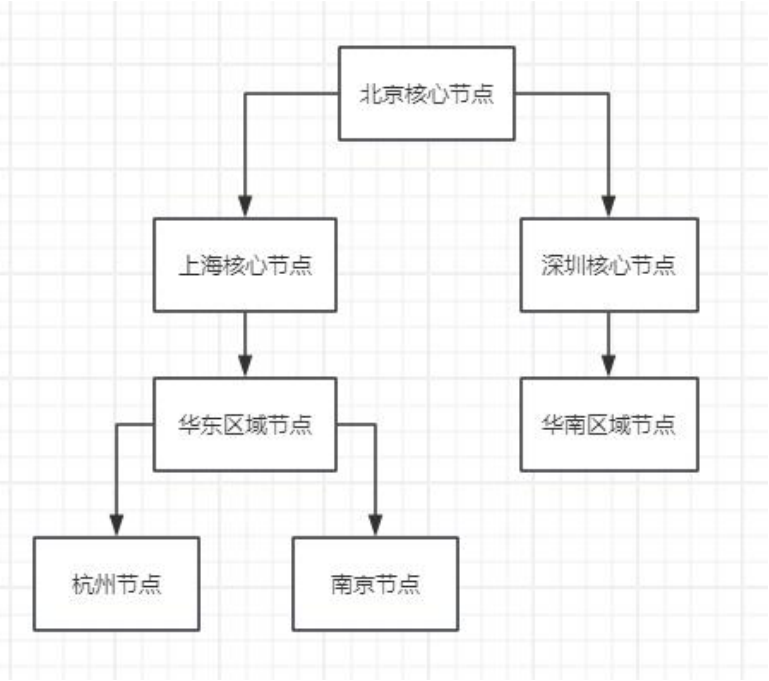

图 3　节点拓扑

8.2 跨链协议集成

8.2.1 数据格式转换工具

——工具功能：

- 支持不同链数据模型的映射转换；
- 自动生成数据转换规则；
- 提供命令行和 API 两种调用方式。

——转换流程：

- 定义源数据模型和目标数据模型；
- 配置字段映射关系；
- 生成转换规则；
- 执行数据转换；
- 验证转换结果。

8.2.2 智能合约迁移方案

——迁移步骤：

- 合约兼容性分析：评估源链合约在目标链的兼容性；
- 代码适配：修改合约代码以适应目标链环境；
- 测试验证：在测试环境中验证合约功能；
- 灰度部署：先在部分节点部署验证；
- 全量迁移：验证通过后全量部署。

——兼容性考虑：

- 共识机制差异：调整合约共识相关逻辑；
- 虚拟机差异：适配目标链的智能合约虚拟机；
- 接口差异：修改合约对外接口调用方式。

8.3 合规与监管对接

8.3.1 监管链数据上报

——上报接口：

- 穿透式接口：支持监管链直接查询业务链数据；
- 数据格式：符合监管链要求的 JSON Schema。

——上报内容：

- 基础数据：交易基本信息、参与方信息等；
- 合规数据：反洗钱相关数据、适当性管理数据等；
- 监管指标：根据监管要求计算的各类指标。

——上报频率：

- 实时上报：重大交易事件发生后 10 秒内；
- 定时上报：每日/每周/每月定时上报。

8.3.2 审计日志留存

——日志内容：

- 系统操作日志：节点操作、配置变更等；
- 交易日志：跨链交易的完整记录；
- 共识日志：共识过程的详细记录。

——留存要求：

- 留存时间：至少留存 60 个月；
- 存储介质：采用一次写多次读（WORM）存储介质；
- 备份策略：异地备份，确保日志不可篡改。

8.3.3 其他司法存证对接

——对接方式：

- 跨链协议对接：通过中继链与司法链对接；
- API 接口对接：提供标准司法取证接口。

——出证流程：

- 取证申请：提交取证需求和相关信息；
- 证据收集：系统自动收集相关跨链证据；
- 证据固化：将证据哈希值上链存证；
- 证书生成：生成符合司法要求的电子证书[4]。

——模板管理：

- 维护多种司法取证模板；
- 支持根据不同司法场景自定义模板。

附 录 A
（规范性）
数据对象 JSON 模式

A.1 数据对象JSON模式示例

```
{
"$schema": "http://json-schema.org/draft-07/schema#",
"title": "证券跨链交易数据",
"type": "object",
"properties": {
"header": {
"type": "object",
"properties": {
"version": {"type": "string", "pattern": "^\\d+\\.\\d+\\.\\d+$"},
"chainId": {"type": "string", "minLength": 3, "maxLength": 10},
"txId": {"type": "string", "pattern": "^\\d{8}\\d{4}$"},
"timestamp": {"type": "string", "format": "date-time"},
"signature": {"type": "string", "minLength": 128}
},
"required": ["version", "chainId", "txId", "timestamp", "signature"]
},
"body": {
"type": "object",
"properties": {
"dataType": {
"type": "string",
"enum": ["SECURITY_TRANSFER", "ACCOUNT_REGISTER", "PRODUCT_ISSUANCE"]
},
"sourceChain": {"type": "string", "minLength": 3},
"targetChain": {"type": "string", "minLength": 3},
"securityCode": {"type": "string", "pattern": "^\\d{6}\\.\\w{2}$"},
"quantity": {"type": "integer", "minimum": 0},
"price": {"type": "number", "minimum": 0, "multipleOf": 0.01},
"clientId": {"type": "string", "minLength": 10}
},
"required": ["dataType", "sourceChain", "targetChain", "securityCode", "quantity", "price"]
}
},
"required": ["header", "body"]
}
```

附 录 B
（规范性）
跨链接口 RPC 规范

B.1 跨链接口 RPC 规范（请求/响应模板）

跨链转账接口：

——请求格式：

```
{
  "header": {
    "version": "1.0",
    "chainId": "string",
    "txId": "string",
    "timestamp": "string",
    "signature": "string",
    "dataType": "string",
    "sourceChain": "string",
    "targetChain": "string"
  },
  "body": {
    "securityCode": "string",
    "quantity": "int",
    "price": "decimal",
    "extData": {}
  }
}
```

——响应格式：

```
{
"jsonrpc": "2.0",
"result": {
"txId": "202507010001",
"sourceTxHash": "0xabc123...",
"targetTxHash": "0xdef456...",
"status": "SUCCESS",
"timestamp": "2025-07-01T09:30:05.000Z"
},
"error": null,
"id": "1"
}
```

附 录 C
（规范性）
测试用例示例

C.1 测试用例（功能/性能/安全测试）

功能测试用例：

表 C.1 功能测试用例

测试编号	测试名称	测试步骤	预期结果
TC-001	跨链转账	从交易链转账 100 股到清算链	转账成功，双方链余额正确更新
TC-002	跨链查询	在监管链查询某客户跨链交易记录	返回正确交易记录
TC-003	合约跨链调用	触发清算链合约调用交易链结算	合约正确执行，结算完成

性能测试用例：

表 C.2 性能测试用例

测试编号	测试名称	测试参数	预期结果
PT-001	并发转账	1000 并发跨链转账请求	TPS≥1000，平均延迟 < 500ms
PT-002	大数据量同步	同步 100 万条跨链交易记录	同步时间 <10 分钟
PT-003	长时间运行	持续运行 72 小时跨链业务	系统无故障，性能无明显下降

安全测试用例：

表 C.3 安全测试用例

测试编号	测试名称	测试方法	预期结果
ST-001	交易篡改测试	尝试篡改已上链交易记录	篡改失败，系统告警
ST-002	节点攻击测试	模拟恶意节点发起攻击	系统能识别并隔离恶意节点
ST-003	隐私泄露测试	尝试获取敏感数据	无法获取完整敏感数据

参 考 文 献

[1] JR/T 0288-2023 银行电子凭证技术规范
[2] JT/T 1517-2024 区块链电子提单数据交互及业务流程
[3] SF/T 0076-2020 电子数据存证技术规范
[4] SF/Z JD0400001-2014 电子数据司法鉴定通用实施规范
[5] JR/T 0314-2024 区域性股权市场跨链技术规范
[6] JR/T 0315-2024 区域性股权市场跨链数据规范
[7] JR/T 0316-2024 区域性股权市场跨链认证安全规范
[8] ISO 20022-2023 金融服务 报文规范