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 001—2025

证券业交互行为区块链存证标准

Blockchain Evidence Storage Standard for Interactive Behaviors in 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

在数字化转型浪潮下，证券行业客户交互行为数据呈现爆发式增长，传统存证方式面临数据篡改风险高、司法举证效率低、跨机构协同难等挑战。区块链技术凭借分布式存储、不可篡改、可追溯等特性，为证券业交互行为存证提供了革命性解决方案。本标准旨在构建一套适用于证券行业的区块链存证体系，通过技术融合与流程规范，实现交互行为数据的全生命周期可信管理，助力行业合规发展与风险防控。

1　背景与适用范围

1.1 行业背景

近年来，证券市场电子化交易占比越来越大，日均客户交互行为数据量急剧增加。传统中心化存证模式在面对高频交互、跨机构协作及监管合规要求时，暴露出数据一致性维护成本高、证据法律效力存疑等问题。区块链技术在证券存证领域的应用已成为行业共识，多家头部券商与交易所已开展试点项目，但缺乏统一标准导致系统兼容性不足、司法对接不畅。

1.2 适用范围

本标准适用于证券行业各类交互行为的区块链存证管理，涵盖证券经纪、投资银行、资产管理等业务场景。具体包括：

——证券经营机构（证券公司、基金公司等）的客户交互行为存证；

——技术服务商提供的区块链存证系统开发与部署；

——监管机构对区块链存证数据的合规性审计与监管。

1.3 例外说明

本标准不适用于：

——非电子化交互行为的存证管理；

——涉密业务场景的特殊存证要求；

——境外证券市场的交互行为存证。

2　技术融合趋势

2.1 区块链技术演进

从 1.0 阶段的比特币单一应用，发展至 2.0 阶段以太坊智能合约，当前证券行业正逐步采用 3.0 阶段的联盟链技术。联盟链在共识效率（TPS 可达 5000+）、权限控制（支持监管节点特权）、隐私保护（零知识证明应用）等方面更契合证券业务需求。

2.2 交互行为管理变革

传统基于日志文件的交互行为记录方式，正逐步向"区块链+智能合约"模式转型。智能合约可实现：

——交互行为自动触发存证（如委托申报提交时实时上链）；

——合规规则内置校验（如反洗钱风险交易自动标记）；

——证据链自动生成（从交互发起至结果反馈的全流程存证）。

2.3 跨领域技术融合

本标准融合以下关键技术：

——密码学：国密 SM2/SM3/SM4 算法；

——分布式存储：IPFS 与区块链链式存储协同；

——司法科技：电子签章系统与区块链存证接口对接；

——监管科技：实时数据上报与智能分析模块集成。

3 行业特殊要求

3.1 可追溯性

——交互行为全流程追溯：从客户终端发起→券商系统处理→交易所响应的全链路存证；

——版本迭代可追溯：存证数据结构变更时保留历史版本记录；

——操作日志可追溯：节点对数据的任何操作均需留痕并上链。

3.2 合规性

——符合《证券法》第 137 条关于客户资料保存的要求（保存期限≥20 年）；

——满足《证券期货业数据分类分级指引》中敏感数据保护要求；

——适配中国证监会《监管科技发展规划》中关于数据报送的规范。

3.3 安全性

——物理安全：存证节点部署于等保三级机房；

——网络安全：采用专线互联与防火墙隔离；

——数据安全：敏感信息全生命周期加密（传输加密+存储加密+展示脱敏）；

——运营安全：7×24 小时监控与应急响应机制。

证券业交互行为区块链存证标准

1 范围

1.1 标准覆盖内容

本标准规定了证券业交互行为区块链存证的以下内容：

——数据规范（元素定义、格式要求、元数据管理）；

——技术架构（分层框架、核心组件、跨层功能）；

——安全要求（加密机制、身份认证、隐私保护）；

——实施流程（系统部署、测试验收、运维监控）；

——监管合规（接口规范、司法出证、合规要求）。

1.2 适用对象（证券机构、技术服务商、监管机构）

——证券机构：证券公司、基金管理公司、期货公司等；

——技术服务商：区块链平台开发商、系统集成商；

——监管机构：中国证监会及其派出机构、司法机关。

1.3 例外说明

——场外交易交互行为存证可参考本标准简化执行；

——非实时交互行为（如邮件沟通）的存证可采用离线哈希上链方式；

——跨境证券业务需同时满足境外监管要求。

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。

GB/T 33190-2016 电子文件存储与交换格式 文书类

JR/T 0184-2020 金融分布式账本技术安全规范[1]

GM/T 0054-2018 信息系统密码应用基本要求

《证券业数据分类分级指引》（中国证券业协会2023年发布）[5]

SF/T 0076-2020 电子数据存证技术规范[3]

SF/Z JD0400001-2014 电子数据司法鉴定通用实施规范[4]

3 术语和定义

3.1 交互行为

指证券市场参与者之间通过电子化方式进行的信息交流与业务处理活动[2]，包括但不限于：

——交易类：委托申报、撤单、成交确认；

——账户类：开户、资料变更、密码修改；

——服务类：咨询问答、投诉处理、风险揭示；

——其他类：信息披露接收、电子合同签署。

3.2 区块链存证

通过区块链技术对交互行为数据进行固化存证的过程，包含：

——时间戳：基于 UTC 时间，精确到毫秒，符合 NTP 时间同步标准；

——哈希值：采用 SHA-256 算法/SM3 杂凑算法对原始数据计算生成的 256 位哈希值；

——链上节点共识：至少需 3/4 以上共识节点确认（含监管节点）。

3.3 智能合约

部署于区块链上的自动化程序，具备：

——触发式存证规则：预设条件满足时自动执行存证操作；

——合规校验逻辑：内置反洗钱、适当性管理等合规检查规则；

——证据封装功能：按司法要求格式打包存证数据。

3.4 存证有效性

符合以下标准的存证数据可被司法机关采信：

——完整性：数据未被篡改，哈希值与上链时一致；

——关联性：能证明交互行为与业务事实的对应关系；

——合法性：存证过程符合法律法规及行业规范。

3.5 链上/链下数据一致性

通过以下机制确保链上链下数据一致：

——实时哈希同步：链下数据变更时实时计算哈希上链；

——定期对账：每日进行链上哈希与链下原始数据比对；

——争议解决：通过多节点共识机制解决数据不一致争议。

3.6 监管链

由监管机构主导建设的区块链系统，具备：

——监管节点特权：可实时获取全量存证数据；

——监管规则植入：内置监管指标计算与预警逻辑；

——跨链对接能力：与券商存证链实现数据互通。

4 缩略语

——DLT：Distributed Ledger Technology 分布式账本技术

——KYC：Know Your Customer 客户身份识别

——AML：Anti-Money Laundering 反洗钱

——API：Application Programming Interface 应用程序接口

——SDK：Software Development Kit 软件开发工具包

——PBFT：Practical Byzantine Fault Tolerance 实用拜占庭容错

——TLS：Transport Layer Security 传输层安全

——IPFS：InterPlanetary File System 星际文件系统

5 总体架构要求

5.1 分层框架

用户层：

——交互场景定义：支持交易、账户、服务等多类标准场景；
——客户终端接入：

- APP 端：支持 iOS、Android 和鸿蒙平台，集成生物识别模块；
- PC 端：兼容 Windows/Mac OS 系统，支持 U 盾硬件加密。

——管理界面：提供可视化存证管理后台，支持权限分级控制。
接入层：
——协议适配：

- FIX 协议：支持证券交易数据交互；
- HTTP/REST：通用 API 接口标准；
- WebSocket：实时消息推送。

——节点权限管理：基于 RBAC 模型，支持多级权限粒度控制；
——数据缓存：采用 Redis 集群，支持 10 万级 TPS 缓存能力。
核心层：
——共识机制：

- PBFT 算法：共识节点数≥7 个，容错节点数≤2 个；
- Raft 算法：用于子链内部共识，选举周期≤500ms；
- 监管节点介入：监管节点拥有数据优先验证权。

——存证数据结构：

```
json
{
  "txId": "2025070100001",
  "opTime": "2025-07-01T09:30:00.000Z",
  "actionType": "ORDER_SUBMIT",
  "dataHash": "a1b2c3d4e5f6...",
  "nodeSign": "sig123456..."
}
```

——智能合约模板：

- 自动触发存证：当委托申报数据通过校验后自动上链；
- 合规校验：内置适当性管理规则（如风险等级匹配检查）。

基础层：
——分布式存储：

- IPFS：非结构化数据（音视频）分片存储，分片大小 1MB；
- 对象存储：结构化数据备份，支持 OSS/S3 兼容接口。

——计算资源调度：基于 Kubernetes 集群或国产信创服务集群，支持弹性扩缩容；
——对等网络：采用 P2P 通信协议，节点连接数≥5 个/节点。

5.2 跨层通用功能

——开发支持：

- BaaS 平台集成：支持蚂蚁链、长安链等主流 BaaS 平台；
- SDK 工具包：提供 Java/Python/Go 多语言 SDK。

——监管审计接口：

- 实时数据上报：采用 WebSocket 等协议，上报延迟≤100ms；

- 审计日志生成：按监管要求格式生成审计报告。

——安全模块：

- 国密算法支持：SM2 用于签名验签，SM3 杂凑算法生成哈希值，SM4 用于数据加密；
- 密钥管理：集成 KMS 密钥管理系统，支持密钥生命周期管理。

6 数据规范

6.1 数据元素定义

必填字段：

——业务场景：

- 客户身份标识：采用 SM4 加密；
- 交互行为类型（枚举值）：

```
ACTION_TYPES = [
"ORDER_SUBMIT",  # 委托申报
"ORDER_CANCEL",  # 撤单
"ACCOUNT_MODIFY", # 账户修改
"RISK_DISCLOSURE", # 风险揭示
# 其他 12 种类型
]
```

- 时间戳：符合 ISO 8601 格式，如 "2025-07-01T09:30:00.000+08:00Z"；
- 原始数据哈希值：采用 SHA-256 算法，哈希值长度 256 字符；
- 存证节点签名：包含节点 ID、签名时间、CA 证书序列号。

扩展字段：

——业务上下文：

- 交易标的：证券代码（如"600000.SH"）、数量、价格；
- 金融属性：交易金额、费率、税额。

——关联日志索引：指向链下日志系统的唯一索引值，格式为"log_20250701_001"。

6.2 数据格式要求

——结构化数据：

- JSON 格式：符合 RFC 8259 标准；
- Protobuf 格式：版本 3.0，支持数据压缩。

——非结构化数据：

- 音视频记录：分片大小 1MB，每片计算 SHA-256 哈希；
- 附件文件：采用 BASE64 编码后计算哈希上链。

6.3 元数据管理

——版本控制：

- 存证模板迭代记录：包含版本号、变更时间、变更内容；
- 数据结构变更日志：保留至少 5 个历史版本。

——数据生命周期：

- 归档策略：超过 1 年的非活跃数据归档至冷存储；
- 司法取证保留期限：按《证券法》要求保留≥20 年[3][4]。

——字典管理：

- 行为类型字典：新增类型同步更新/定期更新（每季度）；
- 业务代码字典：与交易所代码表同步。

6.4 标签体系设计

——客户维度标签：

- 客户风险等级（保守型/稳健型/激进型）；
- 资产规模、投资偏好（高频交易/长期持有）、服务等级等。

——场景维度标签：

- 开户场景、交易场景、风险测评场景、咨询场景、产品购买场景（股票/基金/债券）、投诉处理场景等。

——行为维度标签：

- 委托下单、撤单、资金划转、信息查询、业务办理、风险揭示确认等。

7 安全要求

7.1 加密机制

——传输层加密：

- TLS1.3 协议：支持 AES-256-GCM 加密套件；
- 密钥交换：采用 ECDHE-RSA 算法，密钥更新周期≤24 小时。

——数据存储加密：

- SM4 算法：分组加密模式为 ECB 模式；
- 加密粒度：敏感字段单独加密（如身份证号、银行账号）。

——其他加密：

- 哈希加密：采用 SHA-256 算法，加盐处理（盐值长度 16 字节）；
- 数字签名：使用 SM2 算法，签名长度 64 字节。

7.2 身份认证

——节点准入控制：

- 白名单机制：仅允许注册节点参与共识；
- CA 证书：使用国密局认证的 CA 机构颁发的证书。

——其他身份认证：

- 设备指纹：采集终端硬件信息生成唯一标识；
- 行为认证：分析用户操作习惯进行身份确认。

7.3 隐私保护

——敏感信息脱敏：

- 身份证号：显示前 6 位+后 4 位，中间用*号遮蔽；
- 银行账号：显示前 4 位+后 4 位，中间用*号遮蔽。

——零知识证明：

- 应用场景：监管机构抽查时，证明数据符合特定条件而不泄露具体内容；
- 算法选择：采用 Groth16 证明系统，证明生成时间≤100ms。

——其他隐私保护：

- 数据匿名化：采用 k-匿名技术，k 值≥5；
- 访问控制：基于 ABAC 模型，支持属性级权限控制。

7.4 抗攻击能力

——防重放攻击：

- 唯一事务 ID：每笔交易生成唯一 ID，有效期 24 小时；
- 时间戳校验：请求时间与服务器时间差超过 5 分钟拒绝。

——女巫攻击防护：

- 节点信誉评分：根据节点历史行为计算信誉值；
- 工作量证明：新节点加入需完成轻量级 POW。

——其他抗攻击：

- 智能合约安全：通过形式化验证工具进行漏洞检测。

8 实施与运维

8.1 系统部署

——混合架构：

- 联盟链主网：由券商、交易所、司法机构等组成共识节点；
- 私有化子链：券商内部使用，用于非敏感数据存证。

——节点部署拓扑：

- 券商节点：每个券商部署 3 个节点（主备+热备）；
- 交易所节点：沪深交易所各部署 2 个节点；
- 司法存证节点：司法链部署 2 个节点。

8.2 测试验收

——功能测试：

- 存证完整性验证：通过多节点数据比对，错误率≤0.0001%；
- 智能合约测试：覆盖 90%以上业务场景。

——性能测试：

- TPS 测试：持续 1 小时，平均 TPS≥1000；
- 延迟测试：99%的交易延迟<500ms。

——其他测试：

- 兼容性测试：支持 3 个以上主流区块链平台。

8.3 运维监控

——异常检测：

- 哈希值突变告警：当区块哈希变化超过阈值时触发告警；
- 共识异常告警：节点离线超过 10 分钟触发告警。

——日志审计：

- 链上操作留痕：记录所有节点操作，保留期限≥20 年；
- 审计报表生成：按日/周/月生成审计报表。

——可视化运维平台监控：

- 普米系统扩展。

9 监管与合规

9.1 监管接口规范

——数据上报格式：

- JSON Schema：符合监管机构定义的标准格式；
- 字段要求：包含业务类型、时间戳、哈希值等 20 个必报字段。

——实时/批量模式支持：

- 实时模式：重大交易事件发生后 10 秒内上报；
- 批量模式：每日凌晨 1 点前上报前一日全量数据。

9.2 司法出证流程

——取证包生成：

- 包含内容：时间戳证书、原始数据指纹、节点共识记录；
- 格式要求：符合 SF/T 0076-2020 标准[3]。

——电子签章：

- 符合《电子签名法》要求[3][4]，使用 CFCA 颁发的签章证书；
- 签章流程：存证机构→司法验证中心→公证处三级签章。

9.3 合规性要求

——投资者适当性存证[5]：

- 记录投资者风险承受能力评估过程；
- 保存产品风险等级与投资者匹配记录。

——信息披露留痕：

- 公告推送记录：包含推送时间、接收方、阅读状态；
- 重大信息披露确认：投资者电子签收记录上链。

9.4 外部司法存证对接

——外部司法存证对接方式：

- 跨链协议：采用哈希锁定机制实现证据锚定；
- API 接口：提供标准司法取证接口。

——出证和模板管理办法：

- 出证流程：申请→审核→证据提取→签章→送达；
- 模板管理：维护 10 种以上司法取证模板，支持自定义扩展。

附　录　A
（资料性）
存证数据示例

A.1　存证数据示例（委托交易场景）

```
{
  "txId": "2025070100001",
  "bizScene": "TRADE",
  "clientId": "ENC_20250701_123456",
  "actionType": "ORDER_SUBMIT",
  "opTime": "2025-07-01T09:30:00.000Z",
  "rawDataHash": "a1b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6q7r8s9t0u1v2w3x4y5z6",
  "nodeSign": "sig_20250701_001",
  "caInfo": "CA00120250701001",
  "extendInfo": {
    "securityCode": "600000.SH",
    "quantity": 100,
    "price": 10.50,
    "orderType": "LIMIT",
    "logIndex": "log_20250701_001"
  }
}
```

附 录 B
（规范性）
司法举证流程模板

B.1 司法举证流程设计依据

B.1.1 法律规范

——《人民法院在线诉讼规则》（法释〔2021〕12 号）第 16-19 条关于区块链存证的效力认定规则；
——《中华人民共和国电子签名法》、《中华人民共和国数据安全法》、《个人信息保护法》关于电子数据合法性、安全性的要求。

B.1.2 技术标准

——符合《区块链信息服务管理规定》的存证平台技术要求[6]；
——上证链等符合国家标准的区块链技术规范[6]。

B.1.3 行业实践

——证券行业客户交互行为数据存证场景的特殊性（如适当性管理、风险提示等）。

B.2 司法举证流程框架

B.2.1 数据采集与存证阶段

数据采集与预处理：
——数据源：客户交互行为数据（如业务办理、适当性评估、风险提示、短信/电话记录等）。
——技术要求：

- 通过埋点、API 接口、日志采集等技术实时/定时采集数据；
- 数据脱敏处理（匿名化、去标识化），确保符合个人信息保护要求；
- 数据加密（采用国密算法或 AES-256 等标准加密技术）。

数据上链存证：
——存证平台：基于上证链或其他符合国家标准的区块链平台。
——存证步骤：

- 哈希计算：对原始数据生成唯一哈希值；
- 上链存储：哈希值及关键元数据（时间戳、业务场景标签等）写入区块链；
- 跨链同步：数据副本通过区块链节点分布式存储，确保不可篡改。

存证信息管理：
——存证凭证：生成包含以下内容的电子存证证书：

- 数据哈希值、区块链交易 ID、时间戳、存证平台资质证明；
- 数据来源说明（如采集系统名称、采集时间、操作人员）。

——异常处理：对未成功上链的数据启动异常流程（如日志补传、人工复核）。

B.2.2 举证准备阶段

证据材料整理：

——存证记录：从区块链平台调取相关交易哈希、时间戳及存证证书；
——原始数据：保留加密后的原始交互数据（如通话录音、短信内容、操作日志）；
——技术说明：

- 存证平台的技术架构（如节点分布、共识机制）；
- 数据采集、加密、上链的流程说明。

合规性验证：
——存证平台资质：提供区块链存证服务许可证、信息系统安全等级保护认证；
——数据完整性证明：通过哈希值比对工具验证链上数据与原始数据一致性。

B.2.3 证据提交与审查阶段

法院证据提交：
——提交形式：

- 通过诉讼平台在线提交电子存证证书及技术说明；
- 线下提交公证机构出具的区块链存证公证书（必要时）。

——内容要求：

- 明确数据上链前后的真实性保障措施（如第三方见证、存证平台日志）。

法院审查要点：
——上链后真实性：

- 验证哈希值一致性，确认数据未被篡改（《规则》第 16 条）。

——上链前真实性：

- 审查数据生成机制（如系统日志、操作流程合规性）；
- 验证数据来源是否通过可信环境（如加密采集设备、独立审计记录）。

——存证平台合规性：

- 检查平台是否符合《规则》第 17 条要求（清洁性、安全性、国家标准）[6]。

异议处理：
——异议情形：对方当事人质疑数据真实性或存证平台中立性。
——应对措施：

- 申请专家辅助人出具技术意见（如区块链存证技术原理说明）；
- 提供第三方鉴定机构出具的存证有效性报告；
- 提交存证平台的安全测评报告（如 ISO 27001 认证）。

B.2.4 证据认定阶段

法院认定标准：
——推定有效：符合《规则》第 16 条，区块链存证数据未被推翻。
——排除情形：

- 存证平台与提交方存在利害关系（如自建链未公开节点）；
- 数据生成过程存在人为干预或系统漏洞。

补充举证：
——关联证据：结合其他证据（如客户签字确认书、系统操作日志）形成证据链。
——技术鉴定：委托司法鉴定机构对存证平台及数据完整性进行技术鉴定。

B.3 合规要点总结

B.3.1 技术合规

——采用符合国家标准的区块链存证平台（如上证链）；
——确保数据采集、加密、存储全流程符合《网络安全法》要求。

B.3.2 程序合规

——存证前需明确告知客户数据用途并获得授权（《个人信息保护法》第 13 条）；
——异常数据处理需保留完整日志备查。

B.3.3 举证策略

——提前准备技术说明及第三方认证文件，应对法院对存证平台的审查；
——建立多维度证据体系（区块链存证+原始数据+操作日志）。

B.4 流程图示例

数据采集 → 脱敏加密 → 生成哈希 → 上链存证 → 异常处理
↓
举证准备（存证证书、技术说明） → 法院提交 → 审查（上链后/前真实性）
↓
异议处理（专家意见、鉴定） → 证据认定（采纳/排除）

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] 《证券期货业数据分类分级指引》（中国证券业协会，2023）
[6] 《区块链司法存证应用技术规范》（最高人民法院司法案例研究院，2024）