基于区块链的政法跨部门证据可信流转机制构建与实践

陈　媚

上海商甲信息科技股份有限公司，中国·上海　200030

【摘　要】政法领域跨部门证据流转长期面临真实性难保障、责任追溯难、协同效率低等痛点。本文以某地区政法系统数字化协同项目为实践依托，提出基于区块链的跨部门证据可信流转机制。通过联盟链架构设计、智能合约固化流转规则、隐私计算保障数据安全等技术路径，实现证据从生成、传输到核验的全流程可信管理。实践表明，该机制在行政复议等场景中使证据流转时间缩短 60%，篡改风险降为零，显著提升了政法协同的规范化与高效化水平，为政法领域数字化转型提供了可推广的技术范式。

【关键词】区块链；政法跨部门协同；证据可信流转；联盟链；隐私计算；行政复议

1　引言

1.1 研究背景

在政法跨部门协同工作中，证据作为案件办理的核心要素，其流转效率与可信度直接关系到司法公正的实现和办案质效的提升。然而，传统证据流转模式长期依赖人工交接与纸质存档，存在诸多亟待解决的问题：一方面，真实性难以保障，电子证据易被篡改、纸质证据存在伪造风险，导致跨部门核验时需反复校验，大幅增加了沟通成本；另一方面，责任边界模糊，证据从公安取证、检察院审核到法院采信需经过多个环节，一旦出现问题，难以精准定位责任主体；同时，效率瓶颈突出，跨部门数据壁垒使得证据传输周期冗长，如某类行政案件的证据流转平均耗时长达 72 小时，远超业务规范中对流转时效的要求。

在此背景下，《区块链和分布式记账技术标准体系建设指南》等政策文件的出台，为破解上述难题提供了新的技术路径。区块链技术所具备的不可篡改、分布式共识等特性，能够从技术层面构建可信的证据流转环境。某地区政法系统数字化协同项目正是基于这一思路，积极探索区块链技术在证据跨部门流转场景中的实际应用，旨在通过技术创新提升政法协同工作的规范化与高效化水平。

1.2 研究意义

从技术层面来看，本研究基于某地区政法系统数字化协同项目的实践，构建“区块链+政务协同”的技术框架，重点探索联盟链架构、智能合约与隐私计算的融合应用，能够有效破解多部门间“数据共享需求”与“安全可控要求”之间的固有矛盾，为政法领域跨网、跨域数据协同提供可复用的技术范式。

从实践层面而言，研究通过项目中行政复议证据流转等具体场景，量化分析区块链技术在缩短流转时间、降低篡改风险等方面的实际成效，其验证过程与落地经验可为其他地区政法系统的数字化协同项目提供直接参考，减少同类项目的技术试错成本。

从制度层面来讲，研究结合项目中形成的证据上链规则、权限管控机制等实践成果，推动跨部门证据管理标准化流程的形成，这与“数字政法”建设中“全流程线上闭环”的目标高度契合，能够为政法工作从传统模式向智能化、规范化转型提供制度性支撑。

2　相关技术基础

2.1 区块链核心技术

项目采用联盟链架构，核心技术特性如下：

技术特性	技术实现	在证据流转中的作用
联盟链节点	由政法各部门作为共识节点，共 7 个	实现多部门对证据数据的共同治理与可信校验
不可篡改	采用 SM3 国密哈希算法生成数据指纹	确保证据上链后无法篡改，保留原始状态
智能合约	基于 Solidity 语言开发流转规则脚本	自动执行证据签收、审核、异议处理等流程
跨链交互	通过安全网关与单向光闸实现跨网同步	解决公安内网与政务外网的证据数据互通问题

2.2 隐私计算协同技术

为实现证据共享与隐私保护的平衡，本机制整合两类关键技术：一是数据脱敏技术，针对当事人身份证号、住址

等敏感信息采用掩码处理（如“310********1234”），仅将脱敏后的非敏感数据上传至区块链，确保原始隐私信息不直接暴露；二是安全多方计算技术，在跨部门联合核验证据过程中，依托联邦学习技术构建“数据可用不可见”的协同模式，各部门无需共享原始证据即可完成联合计算与核验，从技术层面规避原始证据泄露风险。

3 证据可信流转机制设计

3.1 总体架构

机制采用“三层架构 + 跨网协同”模式，适配政法系统网络隔离环境：

层级	核心功能	技术组件
基础设施层	节点部署与网络安全保障	区块链一体机、防火墙、安全边界设备
技术支撑层	证据上链与流转控制	联盟链平台、智能合约引擎、隐私计算模块
应用层	业务场景适配	行政复议证据模块、跨部门签收模块等

跨网协同通过“公安侧子链”与“政务侧主链”实现：证据原始数据存储于公安内网，哈希值与元数据通过安全边界同步至政务外网链，确保数据仅在授权范围内流转。

3.2 核心技术机制

3.2.1 证据上链规则

证据上链采用分类处理与共识校验相结合的规则设计。在分类上链策略方面，针对不同类型的证据实施差异化管理：对于结构化证据（如行政处罚决定书等具有固定格式的文书），采用全文上链模式，上链过程中由智能合约自动校验其格式规范性，包括是否包含文号、电子签章等关键要素，确保文书形式符合业务规范；对于非结构化证据（如现场照片、录音等多媒体文件），则仅将其哈希值上链，原始文件通过加密处理后存储于分布式系统，同时将文件名称、生成时间、经办人数字签名等元数据同步上链，既保证证据可追溯性，又降低链上存储压力。

在共识机制层面，采用 PBFT（实用拜占庭容错）算法保障上链过程的可信度。该算法要求证据上链需经过超过 2/3 共识节点的验证认可，通过多节点交叉校验确保上链数据的一致性；同时，其具备容忍部分节点故障或恶意行为的能力，在节点异常情况下仍能维持上链流程的稳定运行，进一步强化证据上链的安全性与可靠性。

3.2.2 智能合约流转控制

设计三类核心合约实现流程自动化：

合约类型	触发条件	执行逻辑
证据提交合约	公安部门上传证据	验证经办人权限→生成上链回执→同步至政务侧链
签收审核合约	司法部门接收证据	记录签收时间→启动 48 小时审核倒计时→超时预警
异议处理合约	接收方提出证据异议	冻结流转流程→推送异议至提交方→双方线上质证

3.2.3 权限与安全管控

权限管理采用三级模型实现精细化管控：提交方（如公安部门）作为证据的初始来源，拥有证据上传权限，且仅可在接收方签收前进行修改操作，确保证据生成后的可控调整；接收方（如司法、检察院等部门）作为证据的流转对象，具备证据查看、签收及审核权限，通过权限边界明确其在协同流程中的核心职能；监管方（如政法委）则承担全流程监督角色，仅拥有审计权限而无修改权限，确保对证据流转过程的合规性把控。

安全防护层面，采用国密 SM4 算法对传输数据进行加密处理，保障跨部门数据交互的机密性；同时，所有操作日志（包括证据上传、修改、签收、审核等行为）均实时上链存证，形成不可篡改的操作轨迹，支持通过 “操作人 - 时间 - 证据标识”多维检索实现全链条追溯，精准定位“谁在何时操作了哪份证据”，从技术层面筑牢安全防线。

4 实践应用与成效分析

4.1 典型场景应用：行政复议证据流转

基于上述机制，某类行政复议案件的证据流转流程得到显著优化。在证据生成环节，由公安部门上传行政处罚决定书等相关证据，系统会自动校验证据格式的规范性（如文书编号、签章信息等），通过校验后即完成上链操作并生成唯一哈希值，确保原始证据的初始状态可追溯。

进入跨网同步阶段，证据的元数据（不含敏感信息）经安全边界（如可信网关、单向光闸）加密处理后，同步至政务外网链，司法部门通过权限验证（如数字证书校验）确认接收后完成签收，整个过程实现跨网络环境的安全数据交互。

在审核与反馈环节，司法部门通过系统在线审核证据内容，若未提出异议，智能合约将自动执行确认流程，完成证据流转闭环；若存在异议，系统会触发异议处理合约，冻结当前流转流程并将异议信息推送至公安部门，双方通过线上质证模块完成争议解决，确保异议处理全程留痕。

案件办结后进入归档追溯阶段，证据流转全流程记录（包括各环节操作人、时间戳、处理结果等）将完整归档

上链，后续可通过案件编号一键调取所有关联信息，实现从证据生成到最终归档的全链条轨迹追溯，满足责任倒查与合规审计需求。

4.2 应用成效

项目实践数据表明，区块链机制应用后成效显著。证据流转平均耗时从传统模式的72小时大幅缩短至28小时，效率提升超六成；证据篡改风险由传统模式年均5起的存在性风险，降至区块链模式下的零风险；跨部门沟通成本从人均2.5小时/案，优化为0.8小时/案，降幅达68%；协同操作满意度也从百分制70分，提升至92分，涨幅31%。

通过数据对比，充分展现区块链在证据管理流程中的优化作用，为政法跨部门协同提供更高效、安全的支撑。

5 结论与展望

5.1 研究结论

本文基于某地区政法协同项目实践，构建了区块链驱动的跨部门证据可信流转机制。该机制通过联盟链架构实现多部门共治，依托智能合约固化流转规则，结合隐私计算平衡共享与安全，有效解决了传统模式下的真实性、效率与责任追溯问题。实践验证表明，区块链技术在政法协同领域具有显著的应用价值。

5.2 未来展望

本机制将进一步推动区块链与人工智能技术的融合应用，通过引入成熟的智能识别与分类算法，实现证据自动分类上链与智能核验，减少人工操作环节，提升证据流转的智能化与高效性。

基于本机制的实践经验，将提炼形成政法跨部门证据流转的技术标准和操作规范，为区域乃至全国的政法协同项目提供统一参考，助力跨域协同工作的规范化、标准化建设。

同时，将持续优化隐私保护策略，结合《数据安全法》《个人信息保护法》等法律法规的最新要求，细化数据脱敏规则与权限管控机制，确保技术应用与制度规范紧密衔接，筑牢数据安全防护屏障。

参考文献：

[1]《全国一体化政务大数据体系建设指南》国办函〔2022〕102号

[2]《区块链和分布式记账技术标准体系建设指南》工信部联科〔2023〕260号

[3]《关于加快推动区块链技术应用和产业发展的指导意见》工信部联信发〔2021〕62号

[4]《上海区块链关键技术攻关专项行动方案（2023-2025年）》沪科〔2023〕292号

[5]《关于发布上海市2024年度区块链关键技术攻关专项项目指南的通知》沪科指南〔2024〕10号

[6]GB/T 42752-2023《区块链和分布式记账技术 参考架构》

[7]GB/T 43572-2023《区块链和分布式记账技术 术语》

[8]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》

[9]GB/T 42570-2023《信息安全技术 区块链技术安全框架》

[10]GB/T 42571-2023《信息安全技术 区块链信息服务安全规范》

[11]GB/T 43574-2023《区块链和分布式记账技术 存证通用服务指南》

[12]GB/T 43577-2023《区块链和分布式记账技术 应用程序接口中间件技术指南》

[13]GB/T 43578-2023《区块链和分布式记账技术 系统测试规范》

[14]GB/T 43575-2023 《区块链和分布式记账技术 跨链技术指南》

[15]GB/T 43576-2023 《区块链和分布式记账技术 隐私保护通用技术要求》

[16]TCCSA 407-2022《基于多方安全计算的数据流通产品技术要求与测试方法》

[17]YD/T 4563-2023《基于联邦学习的数据流通产品技术要求与测试方法》

[18]T/CCSA 406-2022《基于可信执行环境的数据计算平台 技术要求与测试方法》

[19]T/CCSA 410—2022《区块链辅助的隐私计算技术工具 技术要求与测试方法》

[20]YD/T 4690-2024《隐私计算 多方安全计算产品性能要求和测试方法》

[21]YD/T 4692-2024《隐私计算联邦学习产品性能要求和测试方法》

[22]YD/T 4948-2024《隐私计算 可信执行环境产品性能要求和测试方法》

[23]YD/T 4690-2024《隐私计算 多方安全计算产品安全要求和测试方法》

[24]YD/T 4691-2024《隐私计算 联邦学习产品安全要求和测试方法》

[25]YD/T 4947-2024《隐私计算 可信执行环境产品安全要求和测试方法》