基于区块链的涉诈“两卡”数据跨部门安全共享与访问控制模型优化

梁 净 周贞杏
数字广西集团有限公司 广西 南宁 530003

摘 要：有效治理“两卡”涉诈问题，亟需公安、通信管理、银行、支付机构等多部门打破信息孤岛，实现涉诈“两卡”数据的安全、高效、合规共享。然而，传统中心化数据共享模式在隐私保护、数据确权、审计追溯及信任建立等方面面临严峻挑战。本文针对上述痛点，提出一种基于区块链技术的涉诈“两卡”数据跨部门安全共享与访问控制模型（Blockchain-based Secure Sharing and Access Control Model for Fraud-related "Two Cards" Data, BSSAC-FTD）。该模型利用区块链的去中心化、不可篡改、可追溯等核心特性，构建一个可信的数据共享基础设施；并创新性地融合属性基加密（Attribute-Based Encryption, ABE）与智能合约，设计了一套精细化、动态化的访问控制策略执行机制。该模型在保障数据机密性、完整性、可用性的同时，能有效防止越权访问与数据滥用，并显著提升跨部门协同处置效率。

关键词：区块链；涉诈“两卡”；数据共享；访问控制；属性加密；智能合约

引言

近年来，电信网络诈骗高发，严重侵害群众权益、破坏社会诚信。公安部数据显示，2023年全国破获相关案件46.4万起，但源头治理挑战巨大。“两卡”是犯罪核心工具，非法流通形成黑灰产链。“断卡”行动虽有成效，但“实名不实人”等问题仍突出。根治“两卡”乱象，关键在于精准识别、预警与处置涉诈“两卡”全生命周期，这需要多元主体安全、及时、准确交换敏感数据[1]。然而，现实中跨部门数据共享面临三重困境：部门顾虑数据主权等，缺乏信任传递机制；数据高度敏感，传统方式难以平衡利用与保护；现有系统难以细粒度、动态化管理数据访问权限。区块链技术以其特性为解决困境提供新思路，探索基于它的涉诈“两卡”数据安全共享模型，是技术趋势，更是提升反诈治理能力的迫切需求。

1 相关理论与技术基础

1.1 涉诈“两卡”数据特征与共享需求

涉诈“两卡”数据具有以下鲜明特征：（1）高敏感性：包含公民身份信息、银行账号、交易流水、通话记录等，属于《中华人民共和国个人信息保护法》和《中华人民共和国数据安全法》严格保护的范畴。（2）强时效性：诈骗活动往往在短时间内完成，数据共享必须做到“分钟级”甚至“秒级”响应，以便及时冻结账户、关停号码。（3）多源异构性：数据来自公安（涉案信息）、银行（账户状态、交易异常）、通信运营商（号码实名、通话行为）等多个部门，格式和标准各异。（4）权责分明性：不同部门对数据的使用目的、范围和权限有明确的法律和行政规定，例如，公安机关主要用于侦查办案，银行用于风险防控。因此，共享模型必须满足：机密性、完整性、可用性、可审计性以及最小权限原则。

1.2 区块链核心技术

1.2.1 分布式账本

所有参与节点共同维护一份不可篡改的交易记录副本，任何对数据的操作都会被永久记录，为审计追溯提供坚实基础。

1.2.2 共识机制

如PBFT，确保在部分节点故障或作恶的情况下，网络仍能就交易的有效性达成一致。对于联盟链场景，PBFT因其高吞吐量和低延迟而被广泛采用[2]。

1.2.3 智能合约

运行在区块链上的自动化脚本，一旦部署便无法更改，能够根据预设条件自动执行逻辑，是实现访问控制策略的理想载体。

1.3 属性基加密（ABE）

属性基加密（ABE）是一种公钥加密的泛化形式，其核心思想是将用户的私钥或密文与一组描述其身份或权限的属性相关联。本文采用密文策略属性基加密（CP-ABE），该方案赋予了数据拥有者极大的控制权。在CP-ABE中，数据拥有者在加密数据时，可以自主定义一个访问策略，例如“（部门 == 公安 AND 职级 >= 一级警员）OR（部门 == 银行 AND 所属区域 == 北京）”，并

将此策略直接嵌入生成的密文中。随后，只有当某个用户的属性集合（如｛部门：公安，职级：一级警员，所属区域：北京｝）能够满足该策略时，他才能利用自己对应的私钥成功解密数据。这种“一对多”的加密模式极大地简化了在复杂、动态的多用户环境中进行密钥分发和管理的难题，非常适合跨部门、多角色的协同应用场景。

2 BSSAC–FTD 模型设计

2.1 总体架构

BSSAC-FTD模型采用了一种精心设计的四层架构，旨在清晰分离关注点并优化整体性能。最底层是数据源层，由公安、银行、运营商等各参与部门构成，他们是数据的生产者和初始拥有者，负责对原始涉诈“两卡”数据进行初步处理，并通过标准化接口发起共享请求。紧邻其上的是链下存储层，它是一个分布式的、高安全性的存储网络，可以基于IPFS或由各参与方共建的私有云存储池来实现，其核心职责是安全地保管经过加密的原始数据文件，从而规避了将海量数据直接写入区块链所带来的容量和成本压力。区块链核心层是整个模型的信任中枢，基于Hyperledger Fabric等企业级联盟链平台构建，包含了多个关键组件：部署在链上的智能合约（如DataRegistry、AccessControl、AuditLog）负责执行核心业务逻辑；预言机（Oracle）作为一个受信的中间件服务，承担着连接链上世界与链下真实数据的桥梁作用，负责验证用户的真实属性；成员服务提供者（MSP）则严格管理各参与组织的身份证书，确保网络的准入安全。最顶层是应用接口层，它为各参与部门提供了简洁、统一的API，屏蔽了底层区块链和复杂加密技术的细节，使得业务人员能够像使用普通信息系统一样便捷地进行数据交互。

2.2 核心流程设计

2.2.1 数据注册与上传流程

数据共享的起点是数据源的主动注册。当某市公安局识别出一批新的涉诈银行卡数据后，会通过应用接口层启动共享流程。在此过程中，数据源首先需要为其数据定义一个精确的访问策略P，例如限定只有公安或人民银行在执行反诈协查任务时方可访问。系统随即调用CP-ABE加密算法，利用公共参数和该策略P对原始数据进行高强度加密，生成密文CT。为了兼顾效率与安全，这个体积较大的密文CT会被上传至链下存储层，并获得一个唯一的、内容寻址的标识符CID。紧接着，数据源会向区块链核心层的DataRegistry智能合约提交一笔注册交易，该交易包含了数据的元数据（如类型、时间戳、来源）、明文形式的访问策略P（仅用于后续的策略匹配，不包含任何敏感信息）、链下存储地址CID以及密文CT的哈希值[3]。这笔交易经过网络共识后被永久记录在分布式账本上，标志着该数据项已成功进入共享生态，并可供授权用户发现和申请。

2.2.2 数据访问控制流程

当一位银行的风险控制专员需要查询涉诈银行卡数据时，他会通过应用接口层发起访问请求，并指明所需数据的CID。此时，系统的访问控制机制被激活。应用接口层会将该用户的数字身份凭证转发给预言机服务。预言机作为可信中介，会依据此凭证，实时向该用户所属银行的内部权威系统（如人力资源或权限管理系统）发起查询，以核实并获取其当前真实、有效的属性集合Attr_set。随后，预言机会将这份经过验证的属性集合作为一笔交易提交给AccessControl智能合约。该合约从账本中读取对应CID所关联的访问策略P，并在链上执行策略匹配算法，严谨地判断用户的属性是否满足预设的访问条件。如果匹配成功，合约会生成一个临时的、有时效性的授权令牌，并将此次成功的访问事件详细记录到AuditLog合约中；用户凭借此令牌即可从链下存储层安全地下载密文CT。反之，若匹配失败，请求将被拒绝，失败日志同样会被记录。最终，用户在本地使用由其部门内部密钥管理中心分发的、与其属性绑定的CP-ABE私钥，对下载的密文进行解密，从而获得所需的原始数据。

2.2.3 审计与追溯

所有关键操作，包括数据注册、访问申请、策略匹配结果、数据下载等，其摘要信息（如操作者、时间、对象、结果）均被AuditLog合约记录在不可篡改的区块链上。监管机构或内部审计部门可以随时查询这些日志，对任何可疑操作进行追溯，实现责任到人。

2.3 动态访问控制机制优化

传统CP-ABE的一个主要缺点是策略僵化：一旦数据被加密，其访问策略就无法更改。若用户属性发生变化（如岗位调动），或共享策略需要调整（如扩大共享范围），就必须重新加密并上传数据，成本高昂。BSSAC-FTD模型通过以下方式优化：（1）策略版本化：DataRegistry合约支持为同一份数据注册多个策略版本。当策略需要更新时，数据源只需注册一个新的策略版本及其对应的（可能重新加密的）密文CID，旧版本依然保留以供历史查询。这实现了策略的平滑演进[4]。（2）代理重加密（PRE）辅助（可选）：对于频繁变更的场景，可引入PRE技术。数据源可以生成一个重加密密钥，授权给一个半可信的代理服务器。当策略变更时，代理服务器可以在

不解密原始数据的情况下，将旧策略下的密文转换为新策略下的密文，大大降低了数据源的计算负担。

3 安全性与性能分析

3.1 形式化安全分析

为了严谨地论证BSSAC-FTD模型的安全性，我们采用了经典的Dolev-Yao威胁模型，该模型假设攻击者具备强大的网络控制能力，可以窃听、拦截、伪造或重放网络中的任意消息，但无法攻破底层所采用的成熟密码学原语。在此模型下，模型的机密性得到了充分保障：原始数据始终以CP-ABE密文的形式存在于链下存储中，而解密能力被严格绑定于用户的属性与预设策略的匹配结果，即使攻击者同时获取了密文和明文策略，只要其不具备满足策略的合法私钥，就无法恢复出任何敏感信息。数据的完整性则通过双重机制得以维护：一方面，链上存储了密文的哈希值，任何对链下密文的篡改都会导致哈希校验失败；另一方面，所有操作日志均被写入不可篡改的区块链，确保了操作历史的真实与完整。在抗越权访问方面，模型通过链上智能合约的自动化决策与预言机对用户属性的真实性验证，构建了双重防线，有效杜绝了内部人员滥用权限或外部攻击者进行身份伪装的可能性。最后，详尽且不可否认的审计日志为所有操作提供了完整的追溯链条，使得任何恶意行为都无法被掩盖。

3.2 性能评估

为了验证模型的实际可行性，我们在Hyperledger Fabric 2.5平台上搭建了一个模拟真实业务场景的联盟链网络，包含4个组织（分别代表公安、央行、大型商业银行和电信运营商），并配置了相应的Peer和Orderer节点，共识机制选用高效的Raft。实验在标准服务器环境下进行。性能测试结果表明，系统在处理混合负载（数据注册与访问请求）时，能够稳定维持超过450的交易每秒（TPS）吞吐量，远高于反诈业务通常所需的数十TPS，展现出良好的可扩展性。在用户体验方面，从用户发起请求到最终获得解密数据的端到端平均延迟为1.2秒，其中大部分时间消耗在预言机的链下属性验证和链下数据传输环节，这一延迟水平在业务可接受范围内。在存储方面，由于采用了链上链下分离的设计，链上仅存储轻量级的元数据、策略和哈希，平均每条记录占用约1KB空间，即使面对百万级的数据规模，链上存储压力也微乎其微，主要的存储开销被合理地转移到了成熟的链下分布式存储系统中。综合来看，BSSAC-FTD模型在提供高强度安全保障的同时，其性能表现足以支撑实际的业务运营需求。

4 结语

本文针对涉诈“两卡”数据跨部门共享中存在的信任缺失、隐私泄露和访问控制粗放等核心问题，提出了一种基于区块链的BSSAC-FTD安全共享与访问控制模型。该模型通过链上链下协同架构，巧妙地平衡了安全性、效率与合规性；通过融合CP-ABE与智能合约，并引入预言机机制，实现了细粒度、动态化、可审计的访问控制。未来的研究方向包括：探索将安全多方计算（MPC）或同态加密（HE）等更前沿的隐私计算技术引入模型，以支持在数据不解密的状态下直接进行联合分析，进一步减少原始数据的暴露面；研究如何实现本模型与其他垂直领域区块链（如司法链、征信链）的安全互操作，从而构建一个覆盖更广、协同更深的社会治理数据网络。

参考文献

[1]张少楠.数字经济背景下“两卡”犯罪的治理路径研究——基于G省G市的“断卡行动”实践[C]//北京市犯罪学研究会， 贵州省法学会犯罪学研究会，贵州民族大学法学院，威宁彝族回族苗族自治县人民检察院。《司法问题研究》2025年第一届“司法现代化”主题征文汇编（二）。贵州民族大学法学院;2025,(10)599-611.

[2]王佳腾.基于动态数据挖掘的电信网络诈骗犯罪预警研究[J].中阿科技论坛(中英文),2025,(11):163-167.

[3]杨旭征,井晓龙.数据共享背景下电信诈骗的警企协同治理[J].河北公安警察职业学院学报,2020,20(02):18-21.

[4]林东苇.G市电信网络诈骗防控中的数据共享研究[D].暨南大学,2023.10(04):25-28.