工程与管理科学
Engineering and Management Science
第 7 卷◆第 10 期◆版本 1.0◆2025 年
文章类型：论文|刊号（ISSN）：2705-0637(P) / 2705-0645(O)

区块链赋能的继电保护调试数据可信管理与追溯机制

陈华伟
珠海电力建设工程有限公司　519000

DOI：10.12238/ems.v7i10.15724

［摘　要］继电保护是电力系统安全稳定运行的核心防线，其调试数据的可信性与可追溯性直接影响故障诊断精度与系统恢复效率。传统集中式数据管理模式存在单点故障风险、数据篡改隐患及溯源效率低下等问题。区块链技术凭借去中心化、不可篡改、可追溯等特性，为继电保护调试数据管理提供了创新解决方案。本文提出基于区块链的调试数据可信管理与追溯机制，通过分布式账本存储、智能合约自动化执行及动态溯源算法，实现数据全生命周期透明化管理。实验表明，该机制可提升数据完整性验证效率，降低人为干预风险，为电力系统智能化运维提供可靠支撑。

［关键词］区块链技术；继电保护；调试数据管理；数据溯源；智能合约

一、引言

电力系统继电保护装置如同电网的“安全卫士”，通过实时监测电气量变化，在故障发生时快速隔离故障区域，是保障电网安全运行的关键设备。调试数据作为继电保护装置配置与验证的核心依据，包含定值参数、动作逻辑、测试报告等敏感信息，其真实性与完整性直接影响保护动作的可靠性。传统调试数据管理依赖中心化数据库，存在诸多弊端。一方面，单点故障导致数据丢失风险高。例如，2023 年某省电网的调度中心数据库服务器因硬件故障宕机，存储的继电保护调试数据在数小时内无法访问，影响了多个变电站的故障排查进度。当时，由于所有调试数据都集中存储在该服务器上，一旦服务器出现问题，数据就无法及时获取，导致运维人员无法准确判断设备状态，延误了故障处理时间。另一方面，内部人员或外部攻击者可能篡改数据。2024 年某地区电网发生一起内部人员篡改调试数据事件，该人员为掩盖设备维护不当的问题，修改了某变电站继电保护装置的调试记录，导致后续保护动作异常，引发了小范围的停电事故。此外，溯源需依赖人工审计，效率低下且易出错。传统模式下，当需要对调试数据进行溯源时，需要人工查阅大量的纸质或电子记录，不仅耗时费力，而且在记录不完整或存在歧义的情况下，很难准确追溯数据的来源和变更过程。区块链技术通过分布式账本、加密算法与共识机制，构建了一个无需信任的透明化数据生态系统。其不可篡改特性可确保调试数据一旦上链即无法被修改；可追溯性支持从数据生成到使用的全流程审计；智能合约则能自动化执行数据访问规则，减少人为干预。本文提出基于区块链的继电保护调试数据可信管理与追溯机制，旨在解决传统模式的痛点，为电力系统数字化转型提供技术支撑。

二、区块链技术赋能调试数据管理的核心优势

（一）去中心化存储提升数据安全性

传统集中式数据库将数据存储于单一服务器，易成为攻击目标。一旦服务器遭受攻击或出现故障，数据就可能丢失或损坏。而区块链采用分布式存储架构，调试数据被分割为多个区块，由全网节点共同维护。每个节点保存完整账本副本，即使部分节点被攻击，其他节点仍能保障数据完整性。以京东智臻链 BaaS 平台为例，该平台通过部署跨地域节点，在 2024 年抵御了针对某区域节点的 DDoS 攻击。攻击发生时，由于数据分布在多个节点上，攻击者无法通过攻击单一节点来破坏整个系统的数据，确保了供应链数据零丢失。在继电保护场景中，调试数据可存储于电网企业、设备厂商、监管机构等多方节点，形成数据冗余备份。例如，一个大型电网公司可以在其下属的多个变电站、调度中心以及合作的设备厂商处部署区块链节点。当某个变电站的节点出现故障时，其他节点的数据仍然可以正常使用，显著降低单点故障风险。

（二）加密算法保障数据不可篡改

区块链通过哈希函数与非对称加密技术确保数据完整性。每个区块包含前序区块哈希值、时间戳及调试数据指纹，形成链式结构。哈希函数具有单向性和唯一性，任何微小的数据变化都会导致哈希值的巨大改变。若攻击者试图修改某一区块数据，需同步篡改后续所有区块的哈希值，计算复杂度呈指数级增长，理论上不可行。国家电网在 2025 年试点项目中，采用 SHA－3 算法对调试报告进行哈希处理，结合 ECC

加密技术生成数字签名。SHA - 3 算法具有较高的安全性和抗碰撞性，能够为调试数据生成唯一的哈希值。ECC 加密技术则可以为数据提供数字签名，确保数据的来源可信。实验表明，在量子计算模拟环境下，破解 128 位密钥需耗时极长，远超数据有效生命周期。这意味着在当前和可预见的未来，基于这些加密算法的区块链数据具有很高的安全性。

（三）智能合约实现自动化数据管控

智能合约作为区块链上的自动化协议，可嵌入调试数据访问规则。例如，仅允许通过合规性审查的工程师查询高敏感定值参数；当设备状态变更时，自动触发数据更新并通知相关方。南方电网在 2024 年部署的智能合约系统中，将继电保护装置状态监测数据与调试记录关联。当智能传感器检测到装置的电压、电流等参数异常时，智能合约自动冻结对应调试数据并启动溯源流程。以往在这种设备异常情况下，需要人工介入进行数据冻结和溯源，不仅效率低下，而且容易出现人为失误。而智能合约的应用使故障定位时间大幅缩短，提高了电网运维的效率和可靠性。

三、区块链赋能的调试数据可信管理机制设计

（一）系统架构设计

1.数据层

采用 Merkle 树结构存储调试数据哈希值，支持高效验证。Merkle 树可以将大量的数据哈希值组织成一个树状结构，通过验证根哈希值即可快速判断数据是否被篡改。例如，在一个包含多个调试数据块的系统中，只需要计算根哈希值并与预先存储的值进行比对，就可以知道整个数据集合是否发生了变化。

2.网络层

通过 P2P 协议实现节点间数据同步，确保所有节点都能及时获取最新的数据。P2P 协议允许节点之间直接进行通信，无需通过中心服务器，提高了数据传输的效率和可靠性。

3.共识层

选用 PBFT 算法，在保障去中心化的同时满足电力系统对实时性的要求。PBFT 算法能够在较短的时延内达成共识，适合对实时性要求较高的电力系统场景。实验测试表明，该架构在 100 个节点规模下，交易吞吐量可达一定数值，满足继电保护调试数据高频写入需求。例如，在一个大型城市电网中，每天可能会产生大量的调试数据，该架构能够及时处理这些数据的上链操作，保证数据的实时性和完整性。

（二）调试数据上链流程

1.数据采集

通过物联网传感器与调试终端采集电气量、动作时间等原始数据，采用 AES - 256 加密后传输至边缘计算节点。物联网传感器可以实时监测设备的运行状态，采集到的数据经过加密后传输，可以防止数据在传输过程中被窃取或篡改。边缘计算节点可以对数据进行初步处理和分析，减轻中心服务器的负担。

2.数据预处理

边缘节点对数据进行清洗、去重，并生成唯一数据标识符（DID）。例如，某 500kV 变电站调试报告中，将 128 项定值参数编码为 DID - 20250703 - 001 至 DID - 20250703 - 128。数据清洗可以去除采集到的数据中的噪声和错误数据，去重可以避免重复数据占用存储空间。唯一数据标识符可以为每个数据项提供唯一的标识，方便后续的管理和查询。

3.上链存储

预处理后的数据经电网企业节点签名后广播至全网，其他节点验证通过后打包成新区块，并更新 Merkle 树根哈希。电网企业节点的签名可以确保数据的来源可信，其他节点的验证可以保证数据的完整性和合法性。新区块的生成和 Merkle 树根哈希的更新标志着数据正式上链存储。

（三）动态溯源算法实现

为解决传统溯源需遍历全链的问题，本机制引入状态通道技术，将高频访问的调试数据存储于链下，仅将关键状态变更记录上链。溯源时，系统首先定位目标数据所在状态通道，再通过链上记录的通道状态哈希值回溯至初始数据块。例如，在某线路保护装置调试案例中，溯源流程从最新状态通道哈希值出发，经 3 次跳转即可定位至 2024 年 12 月的原始调试记录，耗时较传统方法大幅缩短。状态通道技术可以减少链上的数据存储量，提高系统的性能。同时，通过链上记录的关键状态变更信息，仍然可以实现对数据的完整溯源。

四、实证分析与效果评估

（一）实验环境搭建

基于 Hyperledger Fabric 框架构建测试联盟链，部署 4 个组织节点（电网企业 A/B、设备厂商 C、监管机构 D），模拟继电保护调试数据全生命周期管理。实验数据集包含 2000 份调试报告，每份报告包含 150 - 200 个数据字段。Hyperledger Fabric 框架具有良好的灵活性和可扩展性，适

合构建联盟链应用。通过模拟实际场景中的数据管理和操作，可以更准确地评估区块链赋能的调试数据可信管理与追溯机制的性能和效果。

（二）性能对比分析

性能对比分析显示，区块链模式优势显著。数据完整性验证时间从传统模式的 12.3 分钟大幅缩短至 0.8 秒，提升 99.85%；溯源成功率从 78.5%提升至 100%，提升 27.4%；单次交易成本从 0.02 元降至 0.003 元，降低 85%。实验表明，区块链模式在数据完整性验证效率上提升显著，主要得益于 Merkle 树结构的批量验证能力。Merkle 树可以一次性验证多个数据的哈希值，大大缩短了验证时间。溯源成功率达 100%，得益于链式结构与状态通道的协同设计。链式结构保证了数据的不可篡改和可追溯性，状态通道技术则提高了溯源的效率。交易成本降低得益于联盟链的共识优化。联盟链的共识机制相对简单，减少了计算资源和能源的消耗，从而降低了交易成本。

（三）安全性验证

1.51%攻击

当恶意节点控制 55%算力时，系统自动触发 PBFT 视图切换机制，在 3 个共识轮次内恢复安全状态。PBFT 算法具有较好的容错性，当检测到恶意节点试图控制网络时，会自动切换视图，重新选择合法的节点进行共识，保障系统的安全运行。

2.Sybil 攻击

采用基于 PKI 的节点身份认证体系，有效识别并隔离伪造节点。PKI 体系可以为每个节点颁发唯一的数字证书，通过验证数字证书可以确认节点的身份真实性，防止伪造节点接入网络。

3.智能合约漏洞

通过形式化验证工具 K 框架对合约代码进行静态分析，提前修复重入漏洞与整数溢出风险。形式化验证工具可以对智能合约的代码进行严格的逻辑检查，发现潜在的安全漏洞并及时修复，提高智能合约的安全性。

五、应用挑战与对策建议

（一）技术挑战

数据隐私保护：调试数据中包含商业机密与用户隐私信息，需在透明性与保密性间取得平衡。对策：采用同态加密技术，支持在加密数据上直接进行计算验证。同态加密允许对加密数据进行运算，而不需要先解密，这样可以保护数据的隐私性。同时，引入零知识证明，允许监管机构验证数据合规性而不获取原始内容。零知识证明可以在不泄露数据具体内容的情况下，证明数据满足某些特定的条件。

跨链互操作：电力系统涉及调度、交易、设备管理等多条区块链，需实现数据互通。对策：借鉴京东跨境溯源平台经验，通过中继链技术构建跨链通信协议，支持不同链上调试数据的关联查询。中继链可以作为不同区块链之间的桥梁，实现数据的传输和交互，打破区块链之间的信息孤岛。

（二）管理挑战

标准体系缺失：目前缺乏调试数据上链的统一规范，导致数据格式混乱。对策：由国家电网牵头制定《继电保护调试数据区块链存储标准》，明确数据字段、加密算法及共识机制要求。统一的标准可以规范调试数据的上链流程和管理方式，提高数据的兼容性和互操作性。

人员技能缺口：电网运维人员对区块链技术认知不足。对策：开展“区块链 + 电力”专项培训，2025 年计划培养复合型人才。通过培训可以提高运维人员对区块链技术的理解和应用能力，为区块链技术在电力系统中的推广和应用提供人才保障。

六、总结

区块链赋能继电保护调试数据可信管理与追溯机制意义重大。传统集中式管理存在单点故障、数据易篡改、溯源效率低等弊端。而区块链凭借去中心化、不可篡改、可追溯等特性，通过分布式账本存储、智能合约自动化管控及动态溯源算法，实现数据全生命周期透明管理。实证表明，该机制大幅提升数据完整性验证效率，溯源成功率达 100%，单次交易成本显著降低，有效保障数据安全。未来，可探索量子加密、轻量级客户端及与数字孪生融合，为电力系统智能化运维提供更坚实支撑。

[参考文献]

[1]曹鑫.区块链技术在继电保护调试数据可信管理中的应用研究[J].电力系统自动化，2024.

[2]蒋家运.基于区块链的继电保护调试数据追溯机制设计与实现[J].电力信息与通信技术，2025.

[3]吴要山.区块链赋能下继电保护调试数据安全与隐私保护策略[J].电网技术，2024.