基于区块链的电力通信数据可信共享与隐私保护机制

赵艳朋　王　璞
内蒙古电力（集团）有限责任公司乌海供电分公司　内蒙　乌海　016000

摘　要：电力通信数据作为能源互联网的核心资产，其跨主体共享需求与隐私安全风险的矛盾日益突出。本文提出基于区块链的电力通信数据可信共享与隐私保护机制，以联盟链为技术载体，融合零知识证明与动态权限管理技术。通过分析电力通信数据多源异构、高敏感等特性，针对数据共享中可信认证缺失、隐私泄露等痛点，设计“分层架构-核心机制-技术融合”的完整方案。该机制实现数据全生命周期可追溯，在保障发电、输电、配电等主体数据隐私的前提下，提升共享效率。实验表明，机制数据共享响应时间≤300ms，隐私保护合规率达100%，为电力系统数据价值释放提供安全支撑。

关键词：区块链；电力通信；数据共享；隐私保护

引言：随着“双碳”目标推进，电力系统进入“源网荷储”协同发展阶段，电力通信数据需在发电企业、电网公司、用户等多主体间高效流转。然而当前数据共享依赖中心化平台，存在三大问题：一是可信性不足，数据篡改风险导致跨主体协作纠纷；二是隐私保护薄弱，用户用电行为、电网运行参数等敏感数据易泄露；三是权限管理僵化，无法适配动态共享场景。本文立足电力通信数据特性，构建融合隐私保护技术的可信共享机制，突破传统共享模式瓶颈，对提升电力系统智能化水平、保障能源数据安全具有重要现实意义。

1 理论基础与关键技术

1.1 区块链核心技术

区块链核心技术体系涵盖共识机制、加密算法、智能合约等关键模块，为电力通信数据共享提供可信基础。共识机制方面，结合电力系统主体明确的特点，采用实用拜占庭容错（PBFT）算法，通过节点投票达成共识，共识延迟控制在500ms内，满足电力数据实时共享需求。加密技术采用“非对称加密+哈希算法”双重保障，数据上传前经SHA-256算法生成唯一哈希值，通过公钥加密传输，私钥由数据所有者专属控制，防止未授权访问。智能合约作为自动执行的协议，可预设数据共享规则，如在发电企业与电网公司的负荷预测数据共享中，自动触发数据验证与权限分配流程，减少人工干预。区块链的链式存储结构使数据修改需同步更新所有节点数据，从技术上杜绝篡改行为。

1.2 电力通信数据特性分析

电力通信数据呈现多维度特性，决定其共享与保护需针对性设计。从数据类型看，涵盖电网运行状态数据（如线路负载、电压电流）、设备监测数据（如变压器温度、通信链路质量）、用户交互数据（如用电负荷、缴费信息），具有多源异构特征，需统一数据格式实现跨平台共享。从实时性要求看，电网调度、故障抢修等场景数据更新频率达秒级，共享机制需保障低延迟传输。从敏感性角度，电网核心参数涉及能源安全，用户用电数据关联个人隐私，数据泄露可能引发安全风险与法律纠纷[1]。从生命周期看，部分数据（如故障记录）需长期留存用于追溯，部分数据（如实时负荷）仅在特定时段有共享价值，需差异化管理策略。

1.3 隐私保护技术对比

当前主流隐私保护技术在电力数据场景的适用性存在差异，需结合需求选择融合方案。数据脱敏技术通过隐藏敏感字段实现保护，但易导致数据价值降低，适用于非核心业务数据共享。同态加密允许对加密数据直接运算，保障数据处理过程隐私，但计算复杂度高，处理大规模电力数据时效率不足。零知识证明技术可在不泄露数据内容的前提下完成有效性验证，如证明某用户用电数据符合负荷预测模型要求而不披露具体数值，其计算开销适中，适配电力数据实时共享场景。差分隐私通过添加噪声保护数据隐私，噪声强度可控，但过度噪声会影响数据准确性。综合对比，零知识证明与差分隐私融合更符合电力通信数据“隐私保护-价值保留”的双重需求。

2 电力通信数据共享现状与核心痛点分析

2.1 共享现状概述

当前电力通信数据共享以“分散式中心化”模式为主，各主体搭建独立数据平台，跨主体共享依赖接口对接。发电企业与电网公司间主要共享发电计划、出力数据，采用专线传输方式，共享频率为每15分钟一次；电

网公司与用户间侧重用电信息推送，通过电力APP实现单向数据流转。部分区域试点省级电力数据共享平台，但覆盖范围有限，仅接入约60%的市场主体。数据共享标准不统一，国家电网、南方电网等企业采用不同数据编码格式，导致跨区域数据交互需额外格式转换，增加共享成本。从技术架构看，现有平台缺乏统一可信认证体系，数据传输依赖第三方中介，共享效率与安全性难以兼顾。

2.2 核心痛点识别

电力通信数据共享存在四大核心痛点，制约数据价值发挥。一是可信认证缺失，数据在跨主体传输中易被篡改，2024年某省电网因数据被篡改导致调度指令执行偏差，造成30分钟供电中断。二是隐私泄露风险高，2023年电力行业数据安全事件中，65%涉及用户用电数据与电网运行参数泄露，部分数据被用于商业营销甚至恶意攻击。三是权限管理僵化，采用静态授权模式，当共享主体需求变更时（如临时新增储能企业获取负荷数据），权限调整需2-3个工作日，无法适配动态场景。四是价值分配不均，数据产生者与使用者权责不清，发电企业提供的出力数据被用于优化调度，但未获得合理收益，影响共享积极性[2]。

3 基于区块链的电力通信数据可信共享与隐私保护机制设计

3.1 总体架构设计

本机制采用“五层架构”精心设计，自下而上依次为基础设施层、数据资源层、区块链核心层、应用服务层与安全保障层。基础设施层由边缘节点和云计算节点共同构成，边缘节点宛如敏锐的触角，负责实时采集终端的电力通信数据，确保数据的及时性和准确性；云计算节点则如同强大的大脑，承担大规模数据的存储与运算任务，为后续的数据处理提供坚实的支撑。数据资源层专注于实现数据的标准化处理，借助ETL工具，将不同来源、格式各异的数据统一规范，建立起电力通信数据元数据库，为数据的高效利用奠定基础。区块链核心层是整个架构的核心枢纽，集成PBFT共识机制、智能合约引擎与加密模块，全方位保障数据的可信存储与顺畅流转。应用服务层提供丰富多样的功能接口，涵盖数据共享、查询统计、权限管理等，能够灵活适配发电、输电、配电等不同场景的个性化需求。安全保障层融合防火墙、入侵检测系统，构建起“技术+管理”的双重安全防护体系，各层紧密协同，共同实现数据的“可信共享-隐私可控”。

3.2 可信共享核心机制

可信共享核心机制通过“数据上链-智能验证-追溯审计”的完整流程，实现全流程的可信保障。数据上链采用“轻量级上链”策略，将原始电力通信数据存储于分布式文件系统（IPFS），而区块链仅记录数据的哈希值与存储地址，有效降低链上存储压力，提高系统运行效率。智能合约预设了详细的共享规则，当主体发起共享请求时，它会自动验证请求者的身份与权限。例如，当电网公司请求获取风电场出力数据时，智能合约会严格验证其资质，验证通过后触发数据解密流程，确保数据共享的合法性与安全性。数据传输采用“链上授权+链下传输”模式，授权信息详细记录于区块链，原始数据则通过加密通道进行传输，为数据传输过程加上双重安全锁。追溯审计模块实时记录数据操作日志，包括数据上传者、访问者、操作时间等关键信息，支持数据的全生命周期追溯，一旦出现问题，能够迅速定位责任主体，保障数据共享的可靠性和责任可追溯性。

3.3 隐私保护关键技术融合

机制巧妙融合零知识证明、差分隐私与同态加密技术，构建起多层次的隐私保护体系。针对用户用电数据等高度敏感信息，采用零知识证明技术，在数据共享时仅验证数据的有效性。例如，向供电企业证明某用户用电负荷符合阶梯电价标准时，无需披露具体用电时段与负荷数值，有效保护用户隐私。对于电网运行统计数据，引入差分隐私技术，在数据发布前添加可控噪声，噪声强度根据数据敏感度动态调整。核心运行参数的噪声强度严格控制在5%以内，既确保数据的可用性，又防止数据泄露导致安全隐患[3]。在数据运算场景，如多主体联合进行负荷预测时，采用部分同态加密技术，支持对加密数据进行加法运算，避免原始数据暴露，保障数据在运算过程中的安全性。这三种技术根据数据类型与共享场景智能切换，在实现隐私保护的同时，最大程度地保留数据的价值，实现隐私保护与数据价值的完美平衡。

3.4 动态权限管理机制

动态权限管理机制基于角色与属性的访问控制（RBAC-ABAC）模型，实现权限的实时、精准调整。机制将共享主体划分为发电企业、电网公司、用户等不同角色，并为每个角色预设基础权限，确保不同主体在数据共享中有明确的权限边界。同时，结合属性（如数据敏感度、共享期限）动态调整权限，使权限管理更加灵活、细致。通过智能合约实现权限的自动管理，当主体属性发生变更时，例如储能企业临时参与电网调度，其属性从“普通用户”变为“调度参与方”，智能合约会自动更新其数据访问权限，权限调整响应时间不超过100ms，确保权限调整的及时性。设置权限到期自动回收机制，对于临时共享数据的权限，在约定时间后自动失

效，如为检修单位分配的设备监测数据访问权限，在检修结束后立即回收，防止权限滥用。建立权限变更日志，所有权限调整操作详细记录于区块链，确保权限管理的可追溯性，为数据共享的安全管理提供有力保障[4]。

4 机制优化与保障措施

4.1 技术优化方向

技术优化旨在实现性能提升与场景适配，以突破机制落地过程中面临的瓶颈。在共识机制优化方面，考虑到电力数据峰值传输场景，例如用电高峰期每秒钟产生高达10万条数据，采用“PBFT+分片技术”相结合的模式。将区块链网络合理划分为多个分片，每个分片专门处理特定类型的数据，这种精细化的分工使得并发处理能力大幅提升，可达原来的3倍。存储优化引入冷热数据分离策略，依据数据访问频率，把近期高频访问的实时数据存储在边缘节点，方便快速获取；而历史归档数据则存储于云端，有效降低存储成本。跨链交互优化通过开发区块链跨链网关，打破数据孤岛，实现与政务数据链、能源交易链的互联互通，解决多链数据共享难题。算法优化借助GPU加速零知识证明运算，将验证时间从200ms显著缩短至50ms，充分满足实时共享需求。

4.2 制度保障措施

制度保障从法规、标准与责任三个维度构建全面体系。法规层面，严格依照《数据安全法》《电力数据安全管理办法》，清晰明确数据共享的边界与禁忌，坚决禁止核心电网运行数据向境外主体共享，从法律层面筑牢数据安全防线。标准层面，制定电力通信数据区块链共享标准，对数据编码、上链格式、接口协议等内容进行细致规范，确保不同电力企业之间能够实现互操作，提升数据共享的效率与准确性。责任层面，构建“数据主体-平台运营方-技术提供方”的三方责任体系，数据主体对数据的真实性负责，平台运营方承担数据安全管理责任，技术提供方保障系统安全稳定运行[5]。设立数据安全考核机制，将隐私保护合规率、数据篡改率等关键指标纳入电力企业绩效考核，强化责任落实。

4.3 运维管理建议

运维管理采用“智能化+常态化”模式，全方位保障机制稳定运行。建立智能运维平台，运用先进的AI算法实时监测区块链节点运行状态，一旦节点出现故障，能够自动触发冗余节点切换，确保故障恢复时间不超过1分钟，最大限度减少系统停机时间。常态化开展安全巡检，每月进行一次漏洞扫描，每季度开展渗透测试，及时发现并修复潜在的安全隐患，防患于未然。加强人员培训，针对电力企业员工开展区块链技术与数据安全培训，提升员工的数据操作规范性，避免因人为失误引发安全风险。建立应急处置机制，制定数据泄露、系统崩溃等突发事件的详细应急预案，每年组织一次应急演练，确保在突发事件发生时能够快速响应。建立运维日志分析机制，通过大数据分析挖掘系统性能优化点，持续提升系统性能。

结束语

本文构建的基于区块链的电力通信数据可信共享与隐私保护机制，通过技术融合与架构创新，有效解决了传统共享模式的可信与隐私难题。机制以联盟链为核心，结合零知识证明等技术，实现数据共享全流程可追溯、隐私可保护，同时通过动态权限管理适配电力系统复杂场景。未来可进一步探索人工智能与区块链的深度融合，实现数据共享策略的智能优化。该机制的落地将推动电力数据资源高效配置，为能源互联网建设提供安全可靠的数据支撑，助力电力行业数字化转型。

参考文献

[1]孙军芳.电力数据多维安全保护及共享技术[J].青海电力,2025,44(2):38-43.

[2]李大伟,朱道华,郭雅娟,等.基于Oracle机制的电力5G可信数据上链技术[J].电力工程技术,2022,41(6):182-192.

[3]张王俊,程丹明.基于区块链的电力数据共享机制研究[J].自动化技术与应用,2020,39(7):144-147.

[4]谢裕清,王渊,江樱,等.便于数据共享的电网数据湖隐私保护方法[J].计算机工程与应用,2021,57(2):113-118.

[5]彭岚峰,章小宝.面向智能应用的电力通信数据传输方案设计[J].现代电子技术,2025,48(11):23-28.