

区块链赋能的分布式电力交易智能撮合系统

张怡萱

(国网辽宁省电力有限公司葫芦岛市建昌供电公司)

【摘要】文章提出一种基于区块链技术的分布式电力交易智能撮合系统,通过构建去中心化交易平台,实现供电方与购电方的点对点自主交易,系统整合智能合约、分布式身份认证、加密传输与聚合签名机制,确保交易数据的安全性与可追溯性,同时降低信任成本与交易争议,研究验证了区块链在分布式能源交易中的技术可行性,为能源互联网转型提供了新型基础设施支持。

【关键词】区块链;分布式电力交易;智能撮合;智能合约;去中心化;能源互联网

中图分类号:F426.61;TM73;TP311.13

DOI: 10.13655/j.cnki.ibci.2025.S2.023

Blockchain-powered Intelligent Matching System for Distributed Electricity Trading

ZHANG Yi-xuan

(State Grid Liaoning Power Co., Ltd. Huludao Jianchang Power Supply Company)

【Abstract】This paper proposes a distributed power transaction intelligent matching system based on blockchain technology. By building a decentralized trading platform, it realizes point-to-point autonomous transactions between power supply parties and electricity purchasing parties. The system integrates smart contracts, distributed identity authentication, encrypted transmission and aggregate signature mechanisms to ensure the security and traceability of transaction data, while reducing trust costs and transaction disputes. The research has verified the technical feasibility of blockchain in distributed energy transactions, and provides a new type of infrastructure support for the transformation of the energy Internet.

【Keywords】blockchain; distributed power trading; intelligent matching; smart contract; decentralization; energy Internet

1 引言

能源结构转型下分布式电源、储能设施及用户侧资源大规模接入给传统电力交易模式带来了挑战。传统集中式交易系统普遍存在着数据孤岛,流程低效和信任缺失现象,很难适应分布式能源波动性、随机性和分散性的特点。区块链技术具有去中心化、不可篡改和可追溯等特点,为建立多方协同、数据透明的分布式电力交易生态奠定了技术基础。

2 系统架构分析

2.1 分布式电力交易平台架构

分布式电力交易平台架构为高效电力交易提供了基础支持,核心是建设多主体协同、数据流通畅通和交易流程自动化。该平台包括分布于不同地理位置上的海量发电端、用电端和各种储能设施终端节点^[1]。这些节点利用高速的通信网络,确保数据传输具有低延迟和高可靠性。中心交换节点与每个节点之间的最小带宽可以达到100Mbps,这确保了大量电力数据能够实时传输。分布式电力交易平台主要

由数据采集和预处理层、交易业务逻辑层和用户交互层组成。数据采集及预处理层承担着从各种电力终端设备中获取原始数据的任务,采用数据清洗算法对噪声数据进行清洗以保证数据质量。交易业务逻辑层承载着交易规则制定、交易策略实施和交易风险评估的主要功能。比如,在交易策略的实施上,利用智能算法分析大量历史交易数据,发掘潜在的交易模式以达到更加准确的价格预测以提高交易效益。用户交互层为发电公司、用电用户、电网运营商等各种主体提供了方便的操作界面,支持Web和移动端的访问,确保用户在任何时间和地点都可以参与电力交易,这大大增强了用户的使用体验。

2.2 区块链层和云边的协同机制

区块链层作为分布式电力交易平台信任的基石,通过分布式账本、智能合约和共识算法等关键技术确保电力交易透明、安全和不可篡改,区块链以联盟链方式存在,涉及节点有电力企业和监管机构^[2]。在达成共识的算法中,选择实用拜占庭容错算法(PBFT),此算法在确保交易一致性的基础上,能够

在每秒内处理超过3000笔的交易,极大地促进了交易效率的提升,与传统比特币区块链每秒7次交易相比较,其效率得到了明显提升。智能合约通过代码的方式定义了电力交易的规则,例如交易价格的计算方式和交易时间的限制,并在符合预设条件的情况下自动触发实施,从而减少人为干预和交易纠纷的风险,云边协同机制是一种将云计算强大的计算能力和边缘计算的低延迟优势结合在一起的方法,旨在进一步优化区块链电力交易系统。云端部署有规模庞大的服务器集群来负责储存大量的历史电力交易数据,并进行繁杂的数据分析和建模,如利用机器学习算法预测和分析电力价格走势。该云平台存储容量可达到PB级别,能满足长时间电力交易中对数据存储的要求。边缘端则在电力设备附近部署边缘计算节点对本地设备生成的数据如智能电表实时采集数据等进行实时处理,一旦发现异常用电情况,毫秒级的反应并及时发出报警信号。

3 核心功能模块

3.1 用户身份认证及资质审核

用户身份验证和资质审核模块构成了电力交易安全和可靠的首要防护措施,该模块运用“多因子认证加区块链存证”的技术架构,在身份认证层面,结合生物特征识别(指纹、人脸识别)与动态口令技术,实现用户身份的强校验,误识率低于0.01%,拒绝率控制在1%以内^[3]。同时,引入数字证书机制,基于X.509标准签发电力交易专属数字证书,证书有效期设定为3年,通过在线证书状态协议(OCSP)实现实时吊销与更新,确保证书全生命周期可追溯,资质审核过程依靠区块链不可篡改的特点,对企业营业执照和电力生产/消费许可进行哈希值上链存证,该系统利用自动化规则引擎按照《电力市场准入管理办法》中预设的审核标准,量化评价企业信用评级和产能/用能规模核心指标。例如,发电公司必须满足年度发电量不低于1000万kW·h和环保排放合格率不低于99%的严格要求,一旦审核通过,系统将自动生成相应的链资质标识,与传统的手工审核相比,整个审核流程所需时间不会超过24h,效率提高了80%。

3.2 报价信息管理及交易撮合

关于报价管理,该系统提供了分时报价、阶梯报价等多样化的报价方式,用户可以设置最低报价间隔

为0.01元/kW·h,并且报价的有效期最长可以达到72h。所有的报价信息在经过同态加密后都被保存在区块链上,这不仅确保了用户的隐私,还支持在链上进行验证。数据的加密速度高达100MB/s,能够满足百万用户的并发报价要求,智能撮合引擎采用强化学习算法,综合考虑电价波动、负荷预测、碳减排目标等12类参数,通过Q-learning模型迭代优化撮合策略,在单次撮合中,响应时间不超过500ms,而且撮合的成功率始终保持在98%或更高。该系统支持双向拍卖机制,在发电侧报价和用电侧需求价差大于报价的情况下自动触发报价进行匹配,同时引入博弈论模型对各参与方的利益进行均衡,保证交易价格处于市场出清价的±报价浮动范围之内(见图1)。

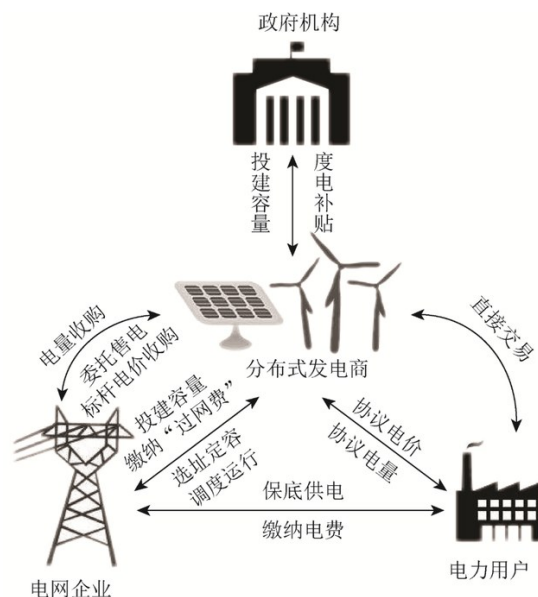


图1 报价信息管理及交易撮合

3.3 交易验证和聚合签名的生成

交易验证和聚合签名生成模块利用区块链共识机制和密码学技术,保证了交易真实性、完整性和不可抵赖性,在交易验证的过程中,使用Merkle树结构对交易数据进行分层哈希处理,这使得单笔交易的验证时间缩短到了50ms,而且验证的准确率达到了100%,该系统能够支持跨链交易的验证,并通过哈希时间锁定合约(HTLC)确保不同的电力交易平台之间的数据交流,同时跨链验证的延迟被限制在2s之内,之后使用BLS(Boneh-Lynn-Shacham)签名策略来生成聚合签名,将多个交易签名整合为一个,签名的长度压缩率高达75%,从而使验证的效率提高

了三倍。在分布式环境下,系统支持门限签名机制,设定3/5签名阈值(也就是五个节点的至少有三个签名是有效的),保障签名过程的安全性与容错性。通过零知识证明技术对全部签名数据进行处理,实现了快速认证,认证吞吐量达到了每秒10万笔数,同时不会泄漏交易敏感信息,符合大规模电力交易实时处理要求(见图2)。

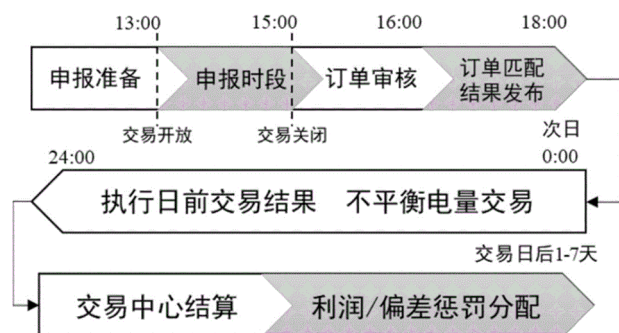


图2 交易验证

4 关键技术的实现

4.1 非对称加密和分布式身份管理

非对称加密和分布式身份管理技术为确保电力交易数据安全和用户隐私提供了核心支持,该系统运用了椭圆曲线加密算法(ECC),并依据NIST推荐的P-256曲线进行加密,其密钥长度达到256位,能够有效抵抗量子计算的攻击,加密强度高达112位对称密钥的安全级别。在进行身份验证的过程中,用户的公私钥生成速度可以达到1000对/s,而签名验证的时间则被严格控制在10ms之内,同时也支持百万级用户的并发操作,分布式身份管理方面,采用去中心化标识符(DID)技术,为每个用户生成全球唯一的DID字符串(如did:web:example.com/user123),关联链上身份凭证。所有的凭证数据都按照可验证凭证(VC)的标准进行存储,这些数据涵盖了企业的资质、信用评级等多方面的信息,每一个VC文件的大小大约是2KB,并且支持快速的数据传输和解析功能。系统通过智能合约实现身份权限动态管理,基于RBAC(角色—权限)模型预设12类角色(比如发电企业、售电公司、监管机构等),误判率低于0.05%,确保身份访问控制的安全性和灵活性。

4.2 改进型的共识算法和交易上链

改进型共识算法和交易上链机制对保证电力交易的高效性和数据一致性具有重要意义。为了解决

传统共识算法在电力交易环境中存在的性能瓶颈问题,该系统引入了经过优化的实用拜占庭容错算法(PBFT),从而将节点间的通信复杂性从 $O(n^2)$ 降低到了 $O(n)$,在100个节点的网络中,共识达成时间从2000ms缩短至300ms,交易吞吐量提升至5000TPS(每秒事务处理量)。该算法采用了动态权重机制,根据节点的历史贡献度和网络的稳定性来分配投票权重,权重的调整周期是每100个区块,这样可以有效地避免恶意节点的攻击,从而将容错率提高到33%。在交易的上链过程中,该系统使用了批量提交的策略,将每50笔交易整合为一个区块,该区块的大小被限制为2MB,打包的时间间隔被设定为10s,从而使得区块的生成效率提高了40%。为了减少存储的负担,采纳状态压缩方法,并使用Merkle Patricia树对过去的交易数据进行存储,从而使存储空间的占用降低了60%。同时,结合侧链技术实现高频小额交易的分流处理,侧链交易确认时间缩短至5s,主链与侧链间通过哈希锁定机制实现跨链数据同步,同步延迟限定为一个区块周期,保证了电力交易数据实时上链和全网一致性。

5 结语

区块链赋能分布式电力交易智能撮合系统,以技术融合解决传统能源交易信任缺失、数据孤岛和流程低效等难题,为分布式能源大规模接入和市场化交易提供技术支持。未来的研究需要进一步优化共识算法的效率和改进监管框架,探索区块链对能源系统暂态分析和稳定性控制方面的深入应用,促进能源互联网朝着更加高效、安全、透明方向发展。

参考文献

- [1] 谢文, 嵇士杰, 纪鹏, 齐宇蓉, 王赢方. 面向能源区块链的分布式电力交易系统的设计[J]. 微型电脑应用, 2024, 40(8): 96-99.
- [2] 张铭泉, 胡俊伟. 面向分布式电力交易的实用拜占庭容错共识算法改进[J]. 电力科学与工程, 2024, 40(10): 58-66.
- [3] 靳松华, 冯恒, 肖嘉豪. 考虑信息误差与隐私保护的分布式电力交易决策[J]. 微型电脑应用, 2025, 41(3): 122-126.