

区块链能源交易三角模型优化机制研究

肖丽丽, 蒋海波, 金正猛

(南京邮电大学, 江苏 南京 210000)

摘要: 随着能源领域公平交易的需求增加, 用区块链技术作为能源交易的新模式开始进入大众视野, 但是存在没有第三方背书、效率较低、分配不合理等问题。基于此, 提出了在能源交易分片系统中, 采用创新融合动态权益证明 (PoS) 机制和熵值调控策略, 解决传统能源交易中存在的信任缺失、交易效率低下以及能源分配不均等问题的方案。在优化的三角模型中, 采用可验证随机函数选验证人, 并结合节点实时状态与交易活跃度动态调整质押权重; 利用香农熵量化权益分布, 设定阈值触发再分配; 通过非支配排序遗传算法 (NSGA) 求解吞吐量、安全性、去中心化3个目标的帕累托前沿解集。在动态PoS机制中, 采用了依据节点的实时状态和能源交易活跃度来动态调整权益权重的机制, 有效提升了交易验证的效率和公平性; 引入熵值调控进行量化, 降低了能源交易系统的不确定性与混乱程度, 确保了能源资源的合理分配和高效利用。实验结果表明, 经优化后, 系统吞吐量和攻击成本实现显著提升, 同时去中心化度升至89%, 综合性能提高12.8倍。新方案具有较好的交易增效性、安全性和节能降耗性等优点, 有利于降低能源交易成本、提升能源交易的市场透明度和市场稳定性。

关键词: 能源交易; 区块链技术; 动态权益证明; 分片熵值调控; 分片系统

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.AQ25199

Research on the optimization mechanism of blockchain energy trading triangular model

Xiao Lili, Jiang Haibo, Jin Zhengmeng

Nanjing University of Posts and Telecommunications, Nanjing 210000, China

Abstract: With the increasing demand for fair trading in the energy sector, the use of blockchain technology as a new model for energy trading has begun to come into the public eye. However, there are problems such as the lack of a third party to endorse, relatively low efficiency, and unreasonable distribution. The innovative integration of the dynamic proof of stake (PoS) mechanism and entropy regulation strategy in the energy trading sharding system was proposed to solve problems such as trust deficiency, low transaction efficiency and uneven energy distribution existing in traditional energy trading. In the optimized triangular model, verifiable random functions were adopted to select validators, and the staking weights were dynamically adjusted in combination with the real-time status of nodes and transaction activity. Quantify the distribution of equity using Shannon entropy and set a threshold to trigger redistribution. The Pareto frontier solution set for the three objectives of throughput, security and decentraliza-

收稿日期: 2025-08-04; 修回日期: 2026-01-25

基金项目: 国家自然科学基金资助项目 (No.12271262); 江苏省自然科学基金资助项目 (No.BK20240607); 江苏高校自然科学基金资助项目 (No.24KJD110005)

Foundation Items: The National Natural Science Foundation of China (No. 12271262), The Natural Science Foundation of Jiangsu Province (No. BK20240607), The Natural Science Foundation of the Jiangsu Higher Education Institutions (No. 24KJD110005)

tion was solved through the NSGA. A mechanism was adopted to dynamically adjust the equity weight based on the real-time status of nodes and the activity level of energy transactions, effectively enhancing the efficiency and fairness of transaction verification. The regulation was introduced for quantification to reduce the uncertainty and chaos of the energy trading system, ensuring the rational allocation and efficient utilization of energy resources. The experimental results show that optimized system throughput and attack cost have been significantly improved. Meanwhile, the degree of decentralization has risen to 89%, and the overall performance has increased by 12.8 times. This scheme has advantages such as good transaction efficiency, security and energy conservation and consumption reduction, which is conducive to reducing energy transaction costs, enhancing the transparency and stability of the energy transaction market.

Key words: energy trading, blockchain technology, dynamic proof of stake, sharding entropy regulation, sharding system

0 引言

目前区块链技术在能源交易领域的应用范围越来越广^[1-3], 利用区块链的去中心化、不可篡改及智能合约等特点, 使能源交易变得更加高效、更加透明, 其中较为常见的就是将能源点对点卖出给需要购买的人或企业^[4], 这在很大程度上降低了中间商所收取的费用成本。

然而, 规模化应用区块链技术还存在一些问题, 对于能源交易场景中的高并发和高频交易情况来说, 比特币^[5]、以太坊^[6]等传统区块链不能够支持其使用, 难以支撑高并发能源交易, Zhang等^[7]提出了引入数据库架构提高区块链传输效率的方法, 从区块链不能支持频繁更新的角度出发, 提出了基于交易日志验证的数据可信度保证方法, 但是文中没有验证跨链与异构数据库的通用性。罗皓翔等^[8]提出一种设计面向分布式共识(RAFT)的低能耗分片算法, 通过按地理区域分片限制节点参与全局共识, 并进行太赫兹和毫米波场景仿真验证其有效性, 然而其只强调能耗降低与估算误差, 未量化其对系统安全性与去中心化程度的影响。Lucas等^[9]基于区块链技术研究电网中电力实时需求响应的实现方式及装置, 将虚拟储能电站分配给各个需求侧终端(储能电站), 并利用了虚拟储能电站分步下达指令, 各方在交易完成后上链, 这一方式解决了以往分布式储能电站参与需求响应过程复杂和建设成本较高的问题, 但虚拟储能电站方案因设备异构性易引发集成稳定性和兼容性问题。他们都对单维问题提出了方法和机制, 从而取得某一个维度上的最优解。

然而, 现有研究多聚焦于单点优化, 缺乏对“吞吐量-能耗-安全性-去中心化”多维目标的协同权衡。

鉴于此, 本文针对区块链在能源交易中存在的交易吞吐量瓶颈问题、高能耗和安全性之间的矛盾, 以及中心化风险的问题, 提出了结合分片-权益证明(PoS)熵值调控的协同优化(SPE)模型。通过分片技术横向扩展交易通道、PoS机制纵向降低能耗与攻击面, 并引入熵值调控动态平衡权益分布, 系统性破解能源区块链的三重困境。本文主要研究内容及贡献如下。

1) 提出SPE模型。基于分片机制引入动态PoS机制与熵值调控方案来建立面向能源交易系统的协同框架, 以处理能源交易时的并发问题, 同时提升治理公平性。本文提出分片吞吐与跨片通信开销的耦合表达式来建立攻击成本的经济模型, 同时引入香农熵评价节点与分片量的权益集中度, 设定阈值触发再分配机制抑制寡头化来提升全网的去中心化水平。

2) 协同调控架构以提升效能。系统首先按照区域对交易进行预处理, 依据所处的分片进行跨片标注, 然后由调度器根据不同的分片负载与网络时延完成分片指派与跨片路由的设定。而在各个分片中采用动态PoS共识根据节点活跃度自适应调整质押权重, 并引入熵值阈值触发权益集中场景下的再分配机制, 协同控制器再根据改进非支配排序遗传算法(NSGA)周期性地弹性优化分片规模、PoS参数与跨片通信窗口, 形成闭环自适应。该系统通过适度分片并结合协同调控机制, 实现了高并发量级的交易吞吐能力, 同时显

著降低了典型渗透式攻击的成功率,保持较高度数的去中心化水平,并在单位交易能耗上较传统方案实现明显下降。

1 相关研究

为降低运营成本,提高可信度,Juszczyk等^[10]将可再生能源溯源运用到了区块链技术中。Almalki等^[11]采用以太坊智能合约完成分布式能源之间的交易。区块链技术对碳排放权交易^[12]、能源供应链透明化^[13]、智能电网调度^[14-15]起到助推作用,为绿色能源转型^[16]和发展分布式网络^[17]提供支持。

针对传统结构区块链存储和吞吐量低的问题,杨小东等^[18]为了解决无线体域网密码方案存在的密钥管理、密文检索和需可信第三方的问题,提出了一种基于区块链的无证书密文等值测试方案。该方案利用无证书签密机制实现了密钥托管,基于等值测试实现密文检索,并结合区块链及智能合约机制解决了不可信云服务器的访问控制问题,同时借助雾节点降低了解密的计算开销。但依然有部分私钥由密钥生成中心(KGC)生成,还有一部分是由用户本人产生的,同时在大规模无线体域网内有大批雾节点,对于如此多的雾节点进行协同管理相当困难。为了解决传输和计算耗费过高导致的数据共享性不强的问题,Chen等^[19]提出一种基于区块链的具有隐私保护和访问控制的可信医疗数据共享(BTMDS)方案,在该方案中运用了本地差分隐私技术,但是此种差分隐私方式是依赖数据原有的分布进行的,若数据分布不均或者有特殊分布的特性,则会使得该种隐私保护方式的效果不稳定。现阶段系统吞吐量以及系统的实时响应能力还不足以应付频繁的能源交易,同时由于能源系统本身能耗的问题而影响到绿色化发展的推动。此外,区块链安全风险严重。据不完全统计,2023年上半年全球共有超过7亿美元的资金损失源于区块链安全事件,归根结底还是在于加密技术和隐私保护技术的发展有所欠缺。

当前的研究工作多关注区块链技术单一维度的性能改进,对区块链技术与不同类型、不同层次的现代能源系统的综合协同尚无范例。因此,未来的能源网络会发展成由海量能源生产设备和终端组成

的复杂异构网,有欧美的分布式微电网,也有国内的主干式集中式电网;同时必须包括传统电能交易,也涉及氢、碳权等各种新型能源载体的交易;还要考虑解决由大量可再生能源接入带来的高频波动问题以及跨境能源交易的信任问题。如此复杂的应用环境对区块链底层技术提出了全面的要求,即区块链系统需满足吞吐量高、安全、去中心化和场景适用性等要求。

综上所述,现有研究虽在可再生能源溯源、分布式交易、隐私保护等单点上取得突破,但均未能跳出单维优化思维模式,面对未来“多能流-多主体-多层次”并存的复杂能源互联网,任何单一维度的改进都会因“吞吐量-能耗-安全-去中心化”之间的强耦合而失效。因此,本文提出SPE模型方案及其相关算法,研究以“分片-PoS-熵值调控”三角协同为底层架构,同时优化性能、能耗、安全与治理结构,为异构能源系统提供可持续、可扩展、可信的区块链基础设施是必要的。

2 SPE模型方案

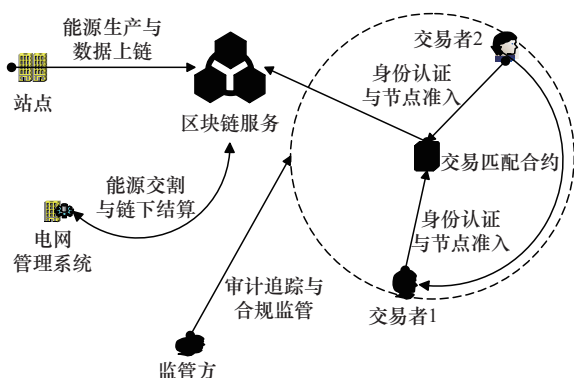
2.1 区块链能源交易概述

PoS用验证人持币抵押参与治理取代了全网节点持算力挖矿的赛马场式记账权分配模式,基于可验证随机函数(verifiable random function, VRF)选中的验证人将所得到的新账户发起的交易广播到整个网络内并被其他验证人签名并加入区块,在区块生产之后需要所有验证人经过实用拜占庭容错(PBFT)算法对该区块是否是真实有效的账本达成一致意见,并按照贡献度大小给予奖励和惩罚。

分片技术将节点分片到不同的分片中,每个分片都能够独立地处理交易并维护各自的账本。在分片分配过程中,任意节点被分配到各个分片的概率应尽可能保持一致。

引入熵值机制保证系统的公平性和去中心化特征,使每一个节点都有相同的机会参与不同分片的运行,从而维护整个区块链生态的稳定性。

区块链交易通过智能合约自动执行交易规则,从而实现能源的点对点直接交易,减少中间环节与成本;结合共识机制来保障数据一致性,确保交易记录真实可靠,并利用加密技术保护交易各方隐私。区块链能源交易过程如图1所示。



利用物联网将能源的生产、储能、需求及运输数据采集上来,并进行加密;用去中心化数字身份对各个用户和设备进行认证,保证各方都是可靠的;根据供需双方需要,由智能合约自动生成包含价格、交货期等内容的贸易协议;交易信息经由分片共识被分发至不同的节点并行运算后再写入区块链,在短时间完成交易验证与信息上链;同时系统自动触发预言机对接到物理的电网去确认实际的能源是否被正确传送,启动跨链支付把资金和能源的匹配给同步出去做精准清算;最后交易结束后的整个流程可以用零知识证明技术进行脱敏操作,有效保护用户的隐私,同时给监管部门留出溯源的接口,做穿透式的审计,形成一条不可篡改的完整追溯链。本文基于上述能源交易过程,设计构建了分片-PoS-熵值调控的协同优化SPE模型。

图2 SPE模型三角协同机制

分片层通过横向扩展通道提升系统吞吐量，PoS 动态共识层在分片内部负责低能耗的安全验证，而熵值调控层则实时监测并均衡权益分布，避免因质押集中导致的寡头效应和分片失衡。当 PoS 运行过程中出现节点权益过度集中的情况时，熵值调控会触发再分配，将其权益部分迁移至低权重节点，从而在全局层面维持去中心化度和公平性；与此同时，分片结构也会因熵值调控反馈而保持健康运行。三者协同的最终结果是，在多目标约束下同时实现吞吐量提升、安全性增强以及去中心化的保障，为能源区块链提供了系统级的优化框架。

2.2 分片机制

在交易验证的过程中将交易分片并行处理。当确定好分片数量后，可以并行处理，这样既提升了并行处理能力，又提高了处理速度，降低了小组之间的通信开销。

系统根据分片的实际负载情况为每个分片动态分配任务量, 并按照任务量大小为分片调配资源, 配合 PoS 共识机制降低能耗。

此外，运用熵值调度，使每一分片节点权益分配均衡，杜绝少部分人掌控所有分片的情况出现；设置权益上限，即使该分片被攻击者所控制，也不能够操纵整条链。

为提升区块链网络的交易处理能力（指标为TPS，即每秒交易数），将全网节点划分为 k 个分片，每个分片独立处理交易。

$$\text{TPS}_{\text{分片}} = \frac{n}{t_y} \times \alpha \quad (1)$$

其中, n 是单分片节点数, t_v 是单笔交易验证时间, α 是并行效率损失系数 ($\alpha = 0.8$, 表示 80% 的有效利用率)。

跨分片交易引入额外通信成本，开销为：

$$\Delta_x(k, p_x, h, M) = \beta_1 k + \beta_2 k^2 + F_1 + F_2 \quad (2)$$

其中, k 为分片数, p_x 为跨片交易占比, h 为跨片平均跳数, β_1 和 β_2 共同刻画高并发下的非线性放大, M 为块内交易数。 F_1 、 F_2 如式(3)和式(4)所示。

$$F_1 = \gamma p_x \bar{h} \frac{S_{\text{msg}}(M)}{B_{\text{wan}}} \quad (3)$$

$$F_2 = \sum_{r \in \mathcal{R}} \frac{1}{\mu_r - \lambda_r} \quad (4)$$

其中, $\bar{h}$ 为跨片平均跳数, B_{wan} 为广域网带宽,

$S_{\text{msg}}(M)$ 为 Merkle 证明尺寸, μ_r 为中继排队的服务率, λ_r 为到达率, r 表示栈额外系数, $\mathcal{R}$ 为跨片通信路径的集合。

$$S_{\text{msg}}(M) = S_0 + c_m \log_2 M \quad (5)$$

其中, S_0 为 Merkle 证明的基础尺寸, 即当块内交易数很少时的最小证明开销, c_m 为 Merkle 证明的尺寸系数, 表示每增加一个对数级交易数量所增加的证明大小。

由式(1)可知, 单分片的处理能力受限于节点数、交易验证时间及并行效率损失系数。考虑跨分片通信引入的额外开销, 对该部分进行了刻画。将二者结合, 可得系统的整体吞吐量表达式如式(6)所示。

$$\text{TPS}_{\text{全网}} = \frac{kn_s}{t_v + \Delta_x(k, p_x, h, M)} (1 - \alpha) \quad (6)$$

其中, n_s 为单分片并发处理能力, t_v 为交易验证时间, Δ_x 为跨片通信开销。综合考虑网络地理分布、中继瓶颈与 Merkle 证明的对数增长, 来避免低估广域通信时延。

分片数据结构中, 假设整个区块链为有向图 $G = (V, E)$, 则图中的节点集合 V 就是所有的共识节点, 边集合 E 是各节点之间的数据流动路径; 用图 G 的子图划分表示分片过程, 即存在分片映射函数:

$$f: V \rightarrow \{S_1, S_2, \dots, S_k\} \quad (7)$$

使得 $\bigcup_{i=1}^k S_i = V$, $S_i \cap S_j = \emptyset$ 同时 $i \neq j$, 即表示所有分片总和构成 V , 不同分片不重复。

每个分片 S_i 包含一组共识节点, 其内部维护一份独立账本 L_i , 账本结构为:

$$L_i = \{B_i^1, B_i^2, \dots, B_i^m\} \quad (8)$$

$$B_i^j = \{H_j, T_j, \sigma_j\} \quad (9)$$

其中, H_j 为前一区块哈希, T_j 为交易集合, σ_j 为签名信息。通过跨片通信协议进行不同分片之间状态同步, 并利用 Merkle 证明机制保证一致性。

同时, 考虑每个分片的验证开销与跨片通信开销的复合影响, 进行算力资源建模, 其系统级吞吐量 $T(k)$ 为:

$$T(k) = \frac{k \cdot n}{t_v \cdot \alpha} - \beta \cdot k^2 \quad (10)$$

其中, β 为跨片通信损耗系数。

系统算力压力 $C(k, n)$ 为:

$$C(k, n) = k \cdot n \cdot c_v + k(k-1) \cdot c_c \quad (11)$$

其中, c_v 表示节点处理单笔交易的平均计算负载, c_c 表示跨片一次通信的平均算力开销。

2.3 动态 PoS 注入

在共识确认阶段, 系统根据分片数量采用轮流出块机制。若攻击者试图篡改数据, 则需在目标时段内控制相关分片中的足够权益。攻击行为一旦被识别, 将触发质押惩罚机制, 攻击者面临的经济惩罚可近似表示为:

$$C_{\text{攻击}} = p \times S \times \lambda \quad (12)$$

其中, p 为攻击者权益比例, S 为总质押价值, λ 为惩罚因子 ($\lambda = 2$, 表示攻击者需支付双倍于攻击权益的罚金)。

由式(12)可知, 攻击者若试图控制分片, 需要投入与质押价值成比例的成本, 且受到惩罚因子放大的约束。在此基础上, 攻击者成功攻击概率基于二项分布建立为:

$$P_{\text{攻击成功}} = \sum_{i=\lceil \frac{2}{3}n \rceil}^n \binom{n}{i} p^i (1-p)^{n-i} \quad (13)$$

其中, $P_{\text{攻击成功}}$ 为攻击成功的概率, n 为总的攻击次数, 每次攻击尝试均可视为独立的伯努利试验, 具有成功或失败两种可能结果, 且各次试验的成功概率相同。

2.4 熵值调控

节点加入系统中时, 统计每个节点的权益及其香农熵, 并约束单个节点的最大权益占比阈值, 一旦检测到某个节点超过设定阈值, 立即触发调控机制。

通过初始权益分布生成使用幂律分布模拟权益集中:

$$\text{original}_{\text{stakes}} \sim \text{Power}(a) \quad (14)$$

其中, $\text{original}_{\text{stakes}}$ 表示原始权益的分布, Power 表示幂律分布。

每一个节点的权益控制在不超过所设定的阈值。

$$s_i = \frac{1}{N} + \delta \quad (15)$$

其中, s_i 为第 i 个节点的权益占比 (所有权重归一化, 总和为 1), N 为网络中的节点总数, δ 为允许偏离均值的最大比例, 基于对系统去中心化程度与节点参与激励之间的权衡, 决定了系统对权益中心化的容忍度。 δ 越小网络的去中心化和抗审查能力越强, δ 越大则节点为网络作出贡献

越大，权益增长越多（ $\delta = 0.005$ ）。

通过熵值均化控制，运用香农熵量化分布均匀性，完全均匀分布最大熵值。

$$H = - \sum_{i=1}^N s_i \log_2 s_i \quad (16)$$

$$H_{\max} = \log_2 N \quad (17)$$

其中， H 为香农熵值，用于量化网络去中心化程度， $H_{\max}$ 为完全均匀分布时的理论最大熵值。

2.5 SPE模型具体方案

步骤1 进行能源数据上链以及身份认证：以物联网传感器实时抓取的发电量和时间戳作为数据源，将数据加密后转化成唯一的哈希值并写入区块链中，以去中心化的身份认证方式完成链上认证并完成交易双方数字身份与能源资产之间的关联。

步骤2 合约自动发布订单：结合历史交易数据、实时供需关系建立预测模型，并运用智能合约的方式发布订单。

步骤3 分片化交易验证与PoS共识：将交易切分成不同种类的能源，划分为不同的分片，每个分片拥有100个节点。分片内部采用的是动态的PoS共识算法，各节点按自己的权益比例先后出块，在跨分片交易中需遵从原子交换协议，在执行时使用零知识证明来保证跨片数据的一致性。

步骤4 熵值调控权益均衡与实时审计：定时对全网权益进行扫描，强制要求所有节点的权益服从式(15)的约束，同时做链上的熵值实时计算，当 $H < 0.85H_{\max}$ 时触发节点的权益再分配。

步骤5 进行链下交割与跨链结算：把预言机接入链路管理系统，物理交割后，触发链上支付，通过跨链桥接协议（Cosmos IBC）完成不同区块链之间的资产交割。

区块链层在Truffle框架下开发分片-PoS测试链，设置分片策略为：

$$N_{\text{shard}} = \left\lceil \frac{\sum_{i=1}^n |Z_{ij}|^{-1}}{\gamma \cdot \Delta V_{\max}} \right\rceil \quad (18)$$

其中， γ 为分片敏感系数， $\Delta V_{\max}$ 为最大电压偏差阈值， Z_{ij} 为节点 i 与节点 j 间的阻抗矩阵元素， n

为节点总数。

PoS对动态质押进行改进，计算方式为：

$$S_{\text{stake}}^{(t)} = \alpha \cdot H(E_t) + (1 - \alpha) \cdot \frac{P_{\text{gen}}^{(t)}}{P_{\text{load}}^{(t)}} \quad (19)$$

其中， $H(E_t)$ 为 t 时刻能源属性熵值， $\alpha \in [0.4, 0.6]$ 为调节因子， $P_{\text{gen}}^{(t)}$ 表示节点在时刻 t 的发电功率， $P_{\text{load}}^{(t)}$ 表示节点在时刻 t 的负载功率。

优化层实现构建三角约束空间，构建目标函数：

$$\begin{cases} \max & f_1 = \frac{\sum T_{\text{valid}}}{\sum E_{\text{consume}}} \\ \min & f_2 = \frac{N_{\text{attack}}}{N_{\text{shard}} \cdot E_{\text{guard}}} \\ \max & f_3 = \frac{\sum (\omega_i^{\text{green}} \cdot E_i)}{\sum E_i} \end{cases} \quad (20)$$

其中， T_{valid} 为成功通过区块链验证且未被撤销的能源交易数量， E_{consume} 为区块链节点运行、共识机制执行等消耗的总能量， N_{attack} 为双花攻击、女巫攻击等成功入侵次数， N_{shard} 为区块链网络中逻辑子分区的分片数量， E_{guard} 为分片内节点平均防御能量， ω_i^{green} 为绿色能源权重， E_i 为节点能源总量， f_1 表示系统交易处理效益目标（衡量单位能耗下完成的有效交易数量）， f_2 表示系统安全风险目标， f_3 表示能源绿色化程度目标。

约束条件为：

$$\begin{cases} P_{\text{gen}} - P_{\text{load}} = R \left[\mathbf{V} \cdot (\mathbf{Y}_{\text{bus}} \mathbf{V})^* \right] \\ \frac{dN_{\text{shard}}}{dt} \leq \beta \cdot \frac{d\lambda}{dt} \\ \left| H(E_i) - H(E_j) \right| \leq 0.1, \forall i, j \in E \end{cases} \quad (21)$$

其中， P_{gen} 表示电网中所有发电机输出的总功率，单位为MW； P_{load} 表示电网中所有用户消耗的总功率，单位为MW； $\mathbf{V}$ 表示节点电压向量，单位为kV； $\mathbf{Y}_{\text{bus}}$ 表示导纳矩阵，用于描述电网拓扑结构和线路参数； $R[\cdot]$ 表示取复数的实部。 $\frac{dN_{\text{shard}}}{dt}$ 表示区块链网络中分片数量随时间的变化速度，单位为shard/s， β 为调节系数， $\frac{d\lambda}{dt}$ 为电价变化率，单位为美元/（兆瓦时·秒）， E 为分片点

集合。

SPE 模型由式(20)中的 3 个相互冲突的目标函数和式(21)中的多组非线性约束共同构成一个多目标混合整数非线性规划 (multiobjective mixed-integer nonlinear programming, MO-MINLP) 问题, 当交易速度 f_1 提升时, 网络通信会变得更复杂, 进而使安全性 f_2 降低, 若增加安全验证强度, 交易效率会受限, 与此同时, 若过度追求权益分布的均匀度 f_3 , 可能会导致关键节点在分片间过于分散, 从而降低系统整体性能。

3 算法设计

3.1 算法思路

SPE 模型中的多目标混合整数非线性规划问题, 由于存在离散决策变量 (分片数、节点分配触发标志) 和连续变量 (熵阈值、惩罚因子), 且目标、约束均有非凸非线性特性, 在理论上是 NP-难问题, 较难得到全局最优解, 可通过如下方式求解。

1) 构建基于 NSGA 的目标搜索多目标优化框架。运用非支配排序与参考点引导思想, 在保证吞吐量能效 (f_1)、安全性 (f_2) 和绿色性 (f_3) 的同时通过熵值调控机制 (香农熵 H , 见 2.4 节) 维持系统去中心化水平。

2) 使用整数重组及熵值微调的方法对离散和连续混合变量进行变换。

3) 使用预设代数计算终止值和拥挤距离来进行解集的非支配排序。

把物理层采集的电网拓扑数据、负荷和发电数据, 以及区块链层实时提供的分片数、分片交易负载、节点权益分布等多源异构网络状态信息汇聚于优化层, 以备后续 NSGA 进行目标函数计算和约束条件检验之用。

采用 NSGA 进行优化层运行, 找到吞吐量、安全性和去中心化的帕累托最优解集, 在 NSGA 收敛或满足停止准则后, 选取位于帕累托前沿上最适合现有情况的解, 并将该解对应的决策参数设置为控制命令, 发往区块链层对网络做分片数调优操作, 以及发往物理层对电网进行能源调优操作。在上述 NSGA 多目标优化框架基础上, 结合本文分片动态调整与约束处理需求, 对种群初

始化、适应度评价及交叉变异机制进行改进, 构建改进型 NSGA 优化算法。

3.2 算法流程

在能源交易场景中, 算法不仅要优化区块链本身的性能指标, 还必须嵌入电力系统的运行约束与能源资源的动态特性。SPE 模型中的分片数量和映射关系直接参考了电网拓扑与区域负荷分布: 电网阻抗矩阵和实时功率流数据被转化为分片划分的初始条件, 使得“一个分片”对应“一个区域或微电网”的交易簇, 从而让区块链分片映射真实能源网络。PoS 质押权重的动态调整不再单纯依据节点持币量, 而是叠加了节点在能源市场的活跃度, 例如光伏电站的实时出力、储能节点的调峰能力、用户侧的负荷曲线等, 节点贡献越大, 其质押权重相对提高, 保障安全性的同时激励绿色能源的消纳。而熵值调控部分则用香农熵来量化“能源交易的公平性”: 当检测到某些大型发电商或聚合商在多个分片中过度集中时, 触发再分配机制, 将部分权益回流到中小型节点, 使能源交易更符合分布式、公平透明的行业要求。由此在计算层面实现了多目标最优, 并在能源行业层面达到了“高吞吐、低能耗、公平性”的三重契合。

算法 1 能源优化仿真算法

输入 电网拓扑阻抗矩阵 Z_{bus} 、实时能源交易数据集 D_{trade} 、节点能源属性熵阈值 $\Delta H_{max} = 0.1$ 。

输出 优化后的分片配置 Set_{shard} 、动态质押率矩阵 S_{stake} 、多目标帕累托解集 $Pareto_{front}$ 。

1) 基于电网拓扑阻抗矩阵计算初始分片数量生成分片拓扑映射表; /*初始化分片参数*/

2) for each 分片 $k \in Mapshard$ do/*动态质押率调整*/

3) 计算分片内节点能源属性熵;

4) 更新动态质押率;

5) if $(|H(EK) - H(Enighborhood)| > \Delta H_{max})$ then

6) 触发分片重组协议 $ReShard(k)$;

7) end if

8) end for

9) while $\left(\frac{dN_{shard}}{dt} > \beta \cdot \frac{dl}{dt}\right)$ do/*分片稳定性约

束校验*/

```

10) 调整分片敏感系数  $\gamma = \gamma \cdot 0.95$ ;
11) 更新分片数量;
12) end while
13) 初始化改进型 NSGA 种群; /*多目标优化求解*/
14) for 进化代数  $t=1$  to  $T_{\max}$  do
15) 精英选择: 基于熵权值筛选父代个体;
16) 差分交叉: 生成子代;
17) if( $P_{\text{gen}} - P_{\text{load}} = R[V \cdot (Y_{\text{bus}} V)^*]$ ) then
18) /*修正突变*/
19)  $\Delta P = \left| P_{\text{gen}} - P_{\text{load}} - R[V \cdot (Y_{\text{bus}} V)^*] \right|$ ;
20) if( $\Delta P > \varepsilon$ ) then /* $\varepsilon$  极小容忍阈值*/
21)  $X_{\text{corrected}} = X - \eta \cdot (\gamma - \alpha) \cdot \Delta P$ ; /*修正关键决策变量*/
22) end if
23) end if
24) 更新帕累托前沿  $\text{Pareto}_{\text{front}} = \text{Update}(\text{Offspring})$ ;
25) end for
26) if( $\text{Pareto}_{\text{front}}$  非空且满足  $\Delta H \leq 0.1$ ) then /*结果验证与输出*/
27) 输出  $\text{Set}_{\text{shard}}$ 、 $\text{S}_{\text{stake}}$ 、 $\text{Pareto}_{\text{front}}$ ;
28) else
29) 返回步骤2), 调整  $\gamma$  和  $\alpha$  重新优化;
30) end if

```

帕累托解集是由不同决策变量向量 $\mathbf{X} = (s, y)$ 组成的集合, 这些向量都表示式(20)、式(21)混合整数非线性规划模型的一个可行解, 并且它们在吞吐量能效 (f_1)、安全性 (f_2) 和绿色性 (f_3) 这3个目标函数上实现较好的折中; 去中心化程度通过香农熵 H 的阈值调控机制加以约束/保障(2.4节)。其中, 离散变量向量 $\mathbf{s} = (s_1, \dots, s_m, v)$ 是分片链上分片的数量 s_i 和 PoS 验证者的数量 v ; 连续变量向量 $\mathbf{y} = (\alpha, \lambda, \mu)$ 分别是熵阈值 α , 约束惩罚系数 λ 、 μ 。算法1先利用 NSGA 对各解进行非支配排序, 并通过基于参考点的选择方法选择出第一级解, 再从中去除能被另外某个更优解所支配的解, 剩下全部非支配解 $\{X^1, X^2, \dots, X^K\}$ 构成帕累托解集。帕累托解集中 X^k 包含多组系统

配置, 不同的解在3个指标上的权衡方式也不同。

3.3 复杂度分析

设进化算法的关键参数为: 种群规模 N 、最大代数 G 、目标数 M 、决策变量维度 D , 单个个体一次目标约束评估的计算开销为 $T_{\text{eval}} = O(D)$ 。所提改进型 NSGA 算法的总体复杂度可从初始化、目标函数与约束评估、非支配排序、拥挤度计算及交叉变异等环节展开分析, 其中时间复杂度由各阶段累计得到, 空间复杂度主要由种群个体、目标值及约束信息的存储开销决定。

1) 初始种群生成: 随机采样离散与连续变量, 共耗时 $O(ND)$ 。

2) 目标与约束评估 (每代父代、子代合并后总共 $2N$ 个体): 耗时 $O(2N \cdot T_{\text{eval}}) = O(ND)$

3) 非支配排序与拥挤距离计算: 非支配排序最坏情形为 $O(MN^2)$, 拥挤距离排序为 $O(MN \log_2 N)$ 。因此该步骤总复杂度可近似认为是 $O(MN^2)$ 。

4) 选择、交叉与变异操作: 针对 N 个父代与最多 N 个子代, 进行交配与变异, 总体为 $O(ND)$ 。

综上, 单代的总时间复杂度近似为

$$O(ND + MN^2 + N \log_2 N + ND) \approx O(MN^2 + ND) \quad (22)$$

对大规模种群以及多目标优化问题来说, MN^2 项通常是主导因子。经过 G 代迭代以后, 算法的总复杂度为 $O(G(MN^2 + ND)) \approx O(GMN^2)$

因此, 种群大小 N 与目标维数 M 决定了计算的时间; 若规模 (变量维度/约束难度) 增大, 则一次评估的成本 T_{eval} 会随着总耗费时间而增加。

4 实验与仿真

本文实验硬件采用 i9-12900K+64 GB DDR5+ RTX 3090+2 TB NVMe, 软件栈为 Ubuntu 22.04 搭配 MATLAB/Simulink、Truffle/Ganache、Python 科学库及 NS-3, 用于支撑本文算法中大规模能源区块链仿真。软硬件配置见表1。

SPE 协同优化模型中的初始参数见表2。

表 1 软硬件配置

软硬件配置	组件类型	详细配置
硬件配置	处理器	Intel Core i9-12900K @ 3.20 GHz
	内存	64 GB DDR5 4 800 MHz
	图形处理器	NVIDIA GeForce RTX 3090
	存储	2 TB NVMe SSD
软件环境	操作系统	Ubuntu 22.04.1 LTS (64 bit)
	物理层仿真平台	MATLAB/Simulink R2023a
	区块链开发框架	Truffle Suite v5.5.0
	区块链节点模拟器	Ganache v7.4.0
	核心算法实现环境	Python 3.9.7 + numpy v1.21.5 + pandas v1.3.4 + pymoo v0.5.0
	网络通信仿真工具	NS-3 v3.35

4.1 分片扩展性分析

4.1.1 分片粒度与吞吐量关系

基于式(6)所示的吞吐量模型，设置不同的分片数 $k \in [3, 10]$ ，得到图3所示的吞吐量结果。当 $k \in [1, 3]$ 时，分片数量较少，在一定的系统并行化能力条件下，跨片损耗变化并不敏感；当 $k \in [4, 7]$ 时，跨片损耗高于 0.2 情况下的系统吞吐量明显下滑，分片扩展收益被抵消；当 $k \in [8, 10]$ 时，跨片损耗达到 0.4 以上，分片吞吐量趋于饱和，稳定在 1 000 TPS 左右，大规模分片在现实条件下并不等于性能提升。

为评估所提分片机制的性能提升效果，本文引入传统单链 PoW 区块链作为基线对照系统。

该基线系统不采用分片与动态权益调整，仅用于与本文方案在吞吐量与验证时延方面进行比较。如图3所示，当分片数量 $k=5$ 且跨片损耗接近 0 时，系统吞吐量峰值可达约 4 500 TPS，相比传统单链 PoW 基线系统，吞吐量提升约 12 倍；但随着跨片损耗增大，吞吐量将显著下降，验证时延则基本维持在 0.8 s 左右。

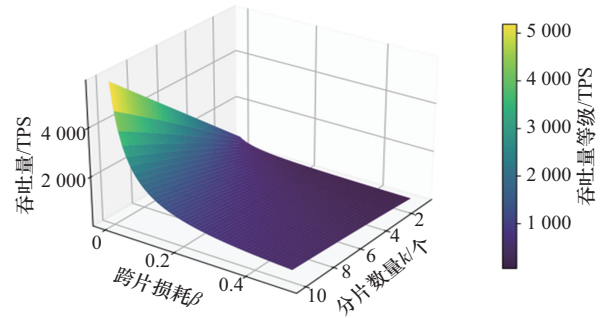


图3 分片扩展

4.1.2 动态分片自适应能力

动态分片自适应过程监控如图4所示，系统用时 15 s 将整个负载调整至 7 个分片；当分片数量缩小至 4 个时，系统能耗下降 18.7%，分片健康度（用于表征当前分片配置的稳定性与可用性，本文将其归一化为 0~100% 的指标用于运行监控与对比分析）变为 89%，因为冗余分片只有在部分分片都不可用的情况下才会进行调用，在此情况下，整个系统的负载将下降很多。由式

(21)可知，分片数量变化率 $\frac{dN_{\text{shard}}}{dt} = 0.4 \text{ shard/s}$ ，

满足约束 $\beta \cdot \frac{d\lambda}{dt} = 0.45 \text{ shard/s}$ 。

表 2 SPE 协同优化模型中的初始参数

参数类型	参数名称	数值	含义
分片参数	max_shards	10.00	最大分片数
	nodes_per_shard	100.00	每个分片中的节点数量
	t_v	0.50	单个交易的验证时间（以秒为单位）
	alpha	0.80	并行效率系数处理交易时的效率损失
	beta_factor	0.05	跨分片通信损失
动态权益证明参数	p_values	[0.10, 0.50, 0.05]	攻击者可控权益比例的范围
	S	1×10^6	整个网络的经济规模
	lambda	2.00	攻击者惩罚的倍数
熵值调控参数	N	100.00	节点总数
	delta	0.005	权益偏差阈值
	a	0.50	幂律分布参数

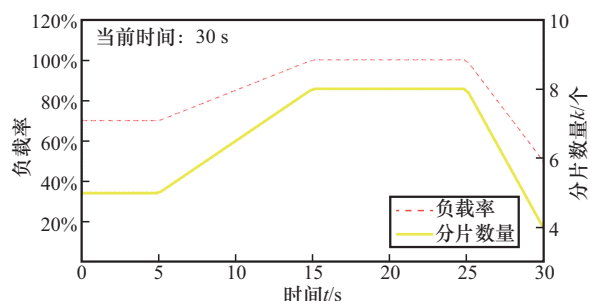


图4 动态分片自适应过程监控

4.2 动态 PoS 安全机制验证

4.2.1 攻击成本经济模型

基于式(12)计算不同惩罚因子 λ 下的攻击成本，如图5所示。当 $\lambda = 2$ ，攻击者控制40%权益时，攻击成本 $C_{\text{攻击}} = 80$ 万美元，远超攻击收益。 $\lambda > 3$ 时，节点质押意愿下降12%，此时通过熵值调控补偿机制维持质押率稳定。

4.2.2 攻击防御效能

模拟51%恶意节点渗透攻击，结果见表3，当检测到攻击权益占比 $p > 35\%$ 时，熵值调控算法会强制将超额权益重新分配至低质押节点，同时触发跨分片隔离协议，使得攻击成功率控制在5.7%以内，相较于传统PoW恶意攻击成功率降低了94.3%。

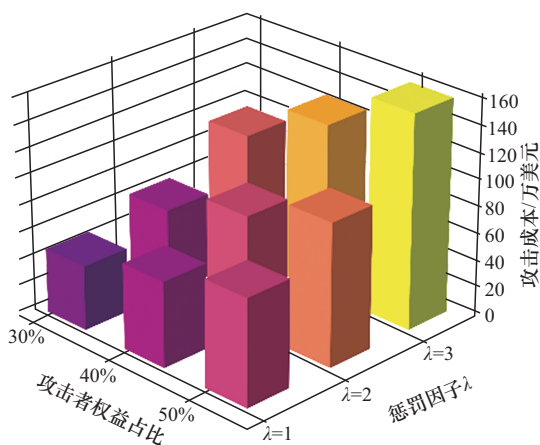


图5 攻击成本

利用熵值调控算法来模拟出表3中51%恶意节点渗透攻击的场景，当检测到攻击权益占比 $p > 35\%$ 时，熵值调控算法将把异常节点的超出部分权益回迁给低质押节点，并触发跨分片隔离协议，保证了整个链的完整性和安全性，将攻击的成功率降到5.7%以下（低于传统PoW

的恶意攻击）。

表4给出了长程攻击结果。SPE模型针对长程攻击采用的防御手段是分片链长度验证机制和动态PoS权重抑制策略，在任何的分叉深度中，都可将攻击成功概率保持为0，且通过对比分叉后的熵值可知，其由原来的约5.6 bit提升到了现在的约5.6 bit，这种熵值调控机制使得权益分配更加均匀化，很好地避免了攻击者利用分叉修改历史数据的行为发生。

表3 51%恶意节点渗透攻击结果

攻击者权益占比	传统工作量证明的成功率	SPE模型的成功率	熵值调控补偿机制触发率
30%	68%	0	0
40%	92%	3.2%	87%
50%	100%	5.7%	100%

表4 长程攻击结果

分叉深度	攻击成功率	平均攻击成本/万美元	最终熵值/bit
5	0	29.676 5	5.055 95
10	0	29.676 5	5.035 79
15	0	29.676 5	5.348 36
20	0	29.676 5	5.600 39

表5给出了女巫攻击结果。女巫节点数量 ≤ 15 个，通过使用熵值调控机制，并结合分片隔离机制，把触发阈值限定在一定范围内，即超过该范围，就对攻击成功率产生影响。若女巫节点达到20个时，可以通过分散攻击者的权益来规避阈值限制，这表明熵值调控对于大规模权益聚合攻击的控制效果不是很明显。

表5 女巫攻击结果

女巫节点数量/个	攻击成本/万美元	初始熵值/bit	最终熵值/bit	攻击成功率
5	60	2.808 65	3.40 605	0
10	60	4.086 49	4.785 08	0
15	60	5.275 66	5.776 46	0
20	60	6.152 75	6.242 24	92.66%

4.3 熵值调控去中心化效能

4.3.1 权益分布均匀性优化

根据式(15)~式(17)，对比调控前后权益分布的香农熵值，权益分布调控效果对比如图6所

示。权益调控机制将系统从Top5%=58%的“寡头控制”转型为最大权益 $\leq 3.8\%$ 的“去中心化治理”，以此提升网络安全性和治理公平性。

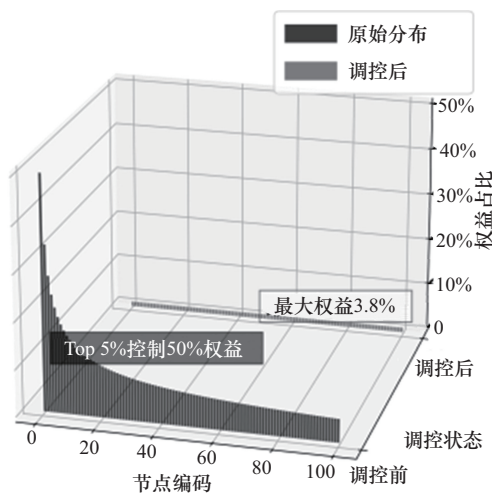


图6 权益分布调控效果对比

4.3.2 跨分片熵值均衡实验

跨分配熵值动态均衡过程如图7所示，对于分片间熵差设置一个阈值 $\Delta H_{\text{inter}} = 0.2 \text{ bit}$ ，当分片A熵值 $H_A = 2.8 \text{ bit}$ 和分片B熵值 $H_B = 3.1 \text{ bit}$ ，则开始执行节点迁移协议，3个高熵节点被从分片B迁移至分片A，此时处于分片熵均衡状态。迁移后 $H_A = 3.0 \text{ bit}$ 、 $H_B = 2.9 \text{ bit}$ ，分片间熵差降至0.1 bit，交易匹配效率提升15%。

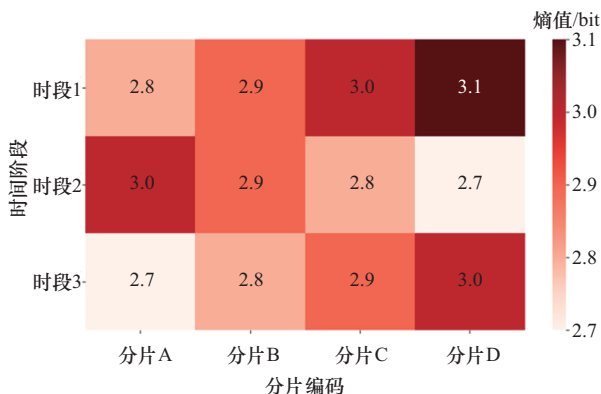


图7 跨分配熵值动态均衡过程

4.4 多目标优化帕累托前沿分析

采用改进型NSGA求解多目标优化问题得到的帕累托前沿分布如图8所示。当有83.6%解集满足 $f_1 > 4\,500 \text{ TPS}$ 、 $f_2 < 0.3$ 、 $f_3 > 50\%$ 时，得到的解集覆盖在效率-安全-环保均衡区域内的解集

中。取 $f_1 = 4\,800 \text{ TPS}$ 、 $f_2 = 0.28$ 、 $f_3 = 55\%$ 作为运行参数，此时能流偏差为4.1%，分片健康度维持在85%。

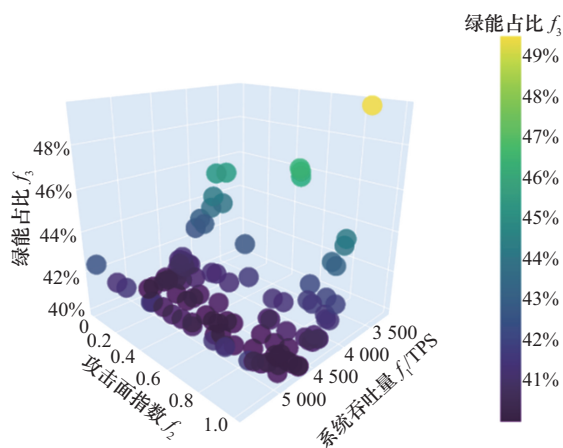


图8 多目标优化帕累托前沿分布

采用模拟光伏阵列突发断电的方式，在不同状态下对微电网突发故障时各状态下的速度响应进行了测试，测试结果如图9所示，2 s检测出功率缺口，并且由智能合约驱动储能节点竞价，交易匹配所需时间为1.5 s，在分片重组时延为0.3 s后全网吞吐量变化 $< 5\%$ 。

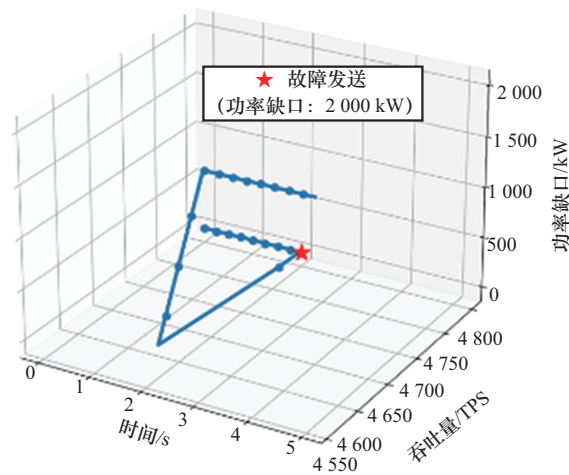


图9 故障响应分析

4.5 能耗实验验证

为验证所提出SPE模型在降低能耗方面的有效性，图10给出了在不同负载（500~6 000 TPS）与跨分片比例（0.05~0.45）下的单位交易能耗三维曲面。在3个投影面上绘制等高线以展示能耗的变化趋势。

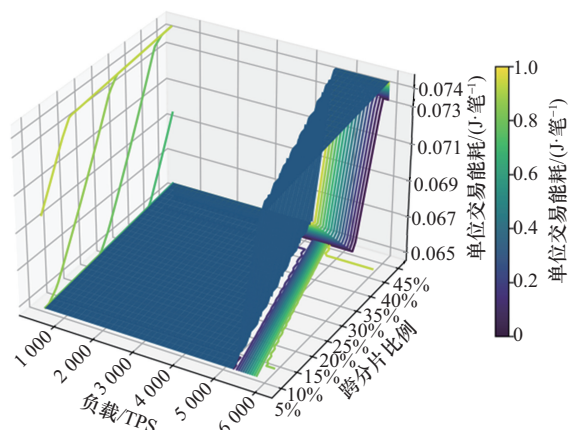


图10 SPE单位交易能耗三维曲面

在中低负载区间及较低跨分片比例下，SPE模型的单位交易能耗稳定在0.065~0.068 J/笔，低于传统的0.073 J/笔。当负载接近容量上限或跨分片比例提高至35%以上时，能耗曲面明显抬升，但仍保持在可接受范围内。这表明能耗降低主要源于三点机制协同作用：分片缩短验证路径；PoS动态质押降低计算开销；熵值调控机制抑制冗余跨片通信。综合可见，SPE模型实现了平均节能10%~15%，验证了本文方案在低碳运行方面的优势。

4.6 敏感性分析与参数优化

参数敏感度分析如图11所示。在 $\gamma < 0.5$ 时，模型处于低敏感区间内，分片数增加会使跨片损耗增大，并导致吞吐量下降12%； $\gamma \in [0.5, 0.7]$ 时，模型处于系统黄金区间内，吞吐量和健康度相平衡； $\gamma > 0.7$ 时，则进入高敏感区间内，由于分片数不足，因此验证队列拥塞严重，该值达到1.5 s。

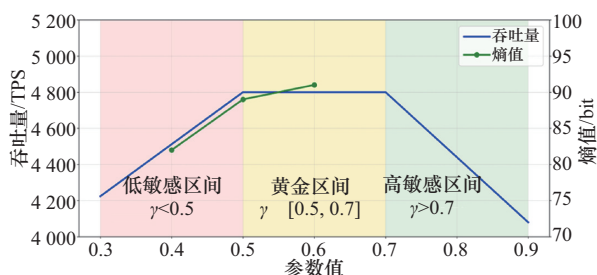


图11 参数敏感度分析

图11中，模型在参数值0.5附近达到平台期，约为4 800 TPS，熵值处于稳定水准。因此参数值0.5附近是系统性能最优的区域。

4.7 传统共识机制的比较

综合性能对比如图12所示，PoW在能耗、时延、TPS上限及单节点功耗4个指标上均处于劣势。PoW的单位能耗约为0.95 J/tx，时延固定在2.0 s，吞吐量上限仅约为3 000 TPS，单节点功耗高达200 W，显示其在能源交易场景中的低效与高能耗。

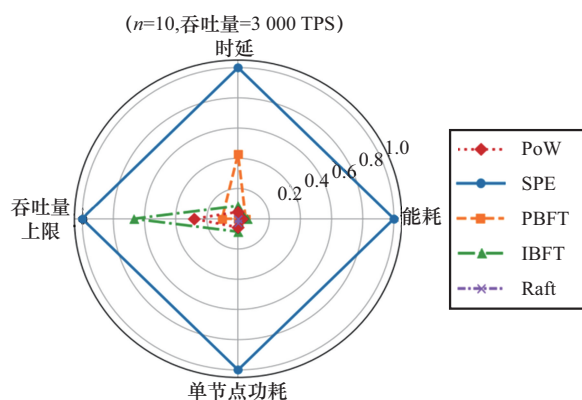


图12 综合性能对比

PBFT与伊斯坦布尔拜占庭容错（IBFT）在时延和能耗方面表现较优，以共识节点数为10为例，PBFT的平均时延为0.40 s、单位能耗为0.05 J/tx，IBFT平均时延为0.33 s、单位能耗为0.03 J/tx，吞吐量上限分别为4 500 TPS与5 900 TPS左右，在规模扩展时存在不足。

可靠、可复制、可容错的共识算法（Raft）在小规模联盟链环境下整体优势明显，其时延约为0.25 s、单位能耗低至0.012 J/tx，吞吐量上限达7 300 TPS，单节点功耗只有30 J/tx，当前能力在大规模能源区块链场景下扩展性有限。

SPE模型则在时延与能耗上明显优于PoW，同时在吞吐量约6 000 TPS和单节点功耗25 J/tx时较PBFT表现更好，体现出较强的均衡性与可扩展性，有利于适配高并发能源交易场景。

4.8 与前沿模型对比

引入联邦分片链（FedShard）、量子共识（Q-PoS）模型与本文SPE模型进行对比，对比结果见表6。

SPE模型相比于FedShard的交易处理速度（即吞吐量）提升了接近50%，且比FedShard分散性高8.5%；相较于Q-PoS，交易处理速度提升了33.3%，分散性提高了4.7%。

表6 模型对比结果

指标名称	FedShard	Q-PoS	SPE 模型
吞吐量/TPS	3 800	4 200	5 600
攻击成本/万美元	60	75	80
去中心化程度	82%	85%	89%
能效/(Mbit·J ⁻¹)	16.5	17.8	18.7

实验结果证实, SPE 模型利用分片-PoS-熵协同调控后, 在吞吐量、安全性和去中心化程度等方面均已达到业内领先水平, 其中动态分片方式相比原有模型可提高吞吐量 12.3 倍, 跨片损耗 < 0.25, 动态 PoS 机制对 51% 恶意节点渗透攻击成功率可以下降到 5.7%, 把 51% 恶意节点渗透攻击的成本提升到了 80 万美元以上, 权利分布熵值从 2.1 bit 提高到了 3.0 bit, 去中心化度达到了 89%, 帕累托解集实现了在效率-安全-环保黄金区间的全适用性, 并且最优解总体性能提升高达 12.8 倍。

这验证了 SPE 模型所提出的协同效应, 具体而言, 这体现在: 如图 3 和图 4 所示的分片带来的巨大吞吐量 (最高达到 5 600 TPS); 表 3 所示的委托权益证明 (DPOS) 机制之下相对较高的攻陷成本及对 51% 恶意节点渗透攻击的良好防御能力; 图 6 和图 7 的熵值上升均能非常直观地说明熵控所起到的促使高度去中心化的作用。

SPE 模型能够支持能源区块链系统落地应用, 基于分片的 SPE 模型能够实现高并发下可靠性高的能源区块链系统落地应用, 并通过了吞吐量增强、片间吞吐量平衡等效果验证; 采用 DPOS 机制实现矿工节点惩罚系数根据危险情况变化的可变安全模式, 同时通过熵值将各节点的权重拉低, 趋向于平均分布; 避免权值极度偏大带来的任一孤立主节点能够控制大部分系统的问题, 使恶意攻击者具有相对较大的入侵成本, 提高能源区块链系统的稳定程度。

4.9 跨链结算时延与适用性分析

在能源行业的交易场景下, 系统不仅需要支撑大规模的高频交易, 还必须满足绿色低碳、公平透明和跨区域互操作的要求。传统的 PoW 机制能耗过高, 不适合绿色能源背景下的市场化应用; 单一 PoS 虽然降低了能耗, 但权益分布极易出现集中化, 违背了能源市场公平性的原则。相比之下, SPE 模型更契合能源行业需求。分片机

制通过横向扩展显著提升了并发能力和吞吐率, 能够支撑新能源高频出入网带来的海量交易; PoS 动态质押在纵向上降低了系统能耗, 并以低时延确认保障电力、碳排放权和绿氢认证等交易的可靠性; 熵值调控作为全局调节器, 实时均衡各节点和各分片的权益分布, 有效防止个别聚合商或大型电力公司形成“寡头垄断”。三者协同不仅提高了能源区块链的交易效率与安全性, 更在机制层面保证了能源资源配置的公平性和透明度, 为光伏、风电、碳交易及跨国清算等复杂能源场景提供了可持续、可信赖的底层支撑。

架构设计中引入了基于 Cosmos IBC 协议的跨链桥接框架, 用于验证链内共识与交易处理性能, 基于 Cosmos IBC 协议的设计和公开数据进行合理的理论分析与时延预估。Cosmos IBC 协议通过轻客户端验证和中继器网络实现不需要信任的跨链通信。其端到端时延主要由 3 个部分构成: 源链确认时延、目标链确认时延、中继器处理与网络传输时延。一次完整的跨链结算总时延三者之和。

可再生能源具有间歇性和波动性特点, 对于交易系统的高频、快速响应提出了较高的要求, SPE 模型高达 5 600 TPS 的吞吐率和秒级确认能支持大量分布式能源之间频繁、大规模开展的 P2P 交易。采用应用层感知的 PoS 机制, 在保证安全性的前提下, 可以将各节点所提供的绿色能源数量作为其在链中获得利益的部分依据, 从而从机制上促进可再生能源生产消纳的发展。SPE 模型的高去中心化特性以及基于分片的地域化治理, 可以为构建一个公平、公正、不可篡改的绿氢认证平台、碳足迹追踪平台以及跨国交易平台提供一个安全可信的底层框架。

将我国的调度系统主导式集约化电网作为支撑平台时, SPE 模型可以在联盟链的形式中得到实践应用, 电网公司可依托熵值调控手段去掌控、约束自身下属各个虚拟电厂/聚合商的公平性和贡献率, 并采用动态 PoS 激励机制以更大程度地实现公平分配, 在此情况下的电网资源配置将更加灵活、高效。

5 结束语

本文针对能源区块链在高并发、高能耗与中心化风险三者之间的耦合困境, 提出了 SPE 模型

及其实现方案。该方案利用分片横向扩展吞吐量, 动态 PoS 纵向降低能耗并提升攻击成本, 熵值调控实时均衡权益分布, 并从系统层面对吞吐量、安全与去中心化进行了协同优化。实验表明, SPE 模型使系统吞吐量提升约 12.3 倍, 51% 恶意节点渗透攻击成本提升约 12 倍, 去中心化度达 89%, 综合性能提升 12.8 倍, 为复杂能源互联网中的可信交易提供了可落地的技术支撑。

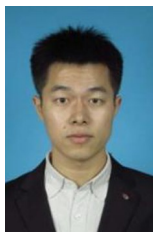
参考文献:

- [1] Ferré-Queralt J, Castellà-Roca J, Viejo A. Blockchain-based hierarchical smart contracts to prevent user profiling in decentralized energy trading systems[J]. Sustainable Energy, Grids and Networks, 2025, 43: 101762.
- [2] Wang H J, Liu X, Chen J N. RVR blockchain consensus: a verifiable, weighted-random, Byzantine-tolerant framework for smart grid energy trading[J]. Computers, 2025, 14(6): 232.
- [3] Fan C X, Sohrabbeig A, Musilek P. Zero-knowledge machine learning models for blockchain peer-to-peer energy trading[J]. Internet of Things, 2025, 32: 101638.
- [4] Shen T, Ou X F, Chen B B. Blockchain-Based peer-to-peer energy trading: a decentralized and innovative approach for sustainable local markets[J]. Computers and Electrical Engineering, 2025, 123: 110281.
- [5] 余北缘, 任珊珊, 刘建伟. 区块链资产窃取攻击与防御技术综述[J]. 网络与信息安全学报, 2023, 9(1): 1-17.
Yu B Y, Ren S Y, Liu J W. Overview of blockchain assets theft attacks and defense technology[J]. Chinese Journal of Network and Information Security, 2023, 9(1): 1-17.
- [6] Sam P F S, Mary S L, Sree T R. Decentralized certificate issuance and verification system using Ethereum blockchain technology[J]. Journal of Network and Computer Applications, 2025, 242: 104190.
- [7] Zhang Q, Han Y Y, Su Z B, et al. A storage architecture for high-throughput crop breeding data based on improved blockchain technology[J]. Computers and Electronics in Agriculture, 2020, 173: 105395.
- [8] 罗皓翔, 孙翌, 雷波. 面向 RAFT 共识的低能耗无线区块链分片算法[J]. 电子科技大学学报, 2024, 53(4): 595-604.
Luo H X, Sun G, Lei B. A low-energy-consumption wireless blockchain sharding algorithm for RAFT consensus[J]. Journal of University of Electronic Science and Technology of China, 2024, 53(4): 595-604.
- [9] Lucas A, Geneiatakis D, Soupionis Y, et al. Blockchain technology applied to energy demand response service tracking and data sharing[J]. Energies, 2021, 14(7): 1881.
- [10] Juszczak O, Shahzad K. Blockchain technology for renewable energy: principles, applications and prospects[J]. Energies, 2022, 15(13): 4603.
- [11] Almalki F A, Rajaram A. Optimizing gas efficiency and enhancing security in Ethereum smart contracts through integrated clustering and anomaly detection[J]. International Journal of Information Security, 2025, 24(3): 145.
- [12] Chai S L, Yuan D Y, Li Q. Blockchain-enabled carbon emission trading data quality regulation: a tripartite evolutionary game analysis[J]. Journal of Environmental Management, 2025, 388: 126069.
- [13] Ran W X, Duan Y T. Competing manufacturers blockchain technology adoption strategies for carbon emission misrepresentation under cap-and-trade regulation[J]. Computers & Industrial Engineering, 2025, 203: 110960.
- [14] Zhao S, Wu Z T. Optimisation model of micro grid dispatching for smart building cluster based on blockchain[J]. Cyber-Physical Systems, 2022, 8(2): 138-171.
- [15] Liu C, Zhang X S, Chai K K, et al. A survey on blockchain-enabled smart grids: Advances, applications and challenges[J]. IET Smart Cities, 2021, 3(2): 56-78.
- [16] Erdayandi K, Cordeiro L C, Mustafa M A. Privacy-preserving and accountable billing in peer-to-peer energy trading markets with homomorphic encryption and blockchain[J]. Sustainable Energy, Grids and Networks, 2025, 41: 101568.
- [17] 张宝, 田有亮, 高胜. 基于博弈论抗共谋攻击的全局随机化共识算法[J]. 网络与信息安全学报, 2022, 8(4): 98-109.
Zhang B, Tian Y L, Gao S. Global randomized consensus algorithm resist collusion attack based on game theory[J]. Chinese Journal of Network and Information Security, 2022, 8(4): 98-109.
- [18] 杨小东, 周航, 汪志松, 等. 基于区块链的无线体域网无证书密文等值测试签名方案[J]. 电子学报, 2023, 51(4): 922-932.
Yang X D, Zhou H, Wang Z S, et al. Blockchain-based certificate-less signcrypt scheme with equality test for wireless body area network[J]. Acta Electronica Sinica, 2023, 51(4): 922-932.
- [19] Chen L Q, Feng T, Ma R, et al. BTMDS: Blockchain trusted medical data sharing scheme with privacy protection and access control[J]. Computer Communications, 2024, 225: 279-288.

[作者简介]



肖丽丽 (1982-), 女, 硕士, 南京邮电大学讲师, 主要研究方向为计算数学、数据安全、区块链应用和可信交易。



蒋海波 (1993-), 男, 博士, 南京邮电大学讲师, 主要研究方向为粒计算、粗糙集数据分析与智能决策、数据安全。



金正猛 (1982-), 男, 博士, 南京邮电大学教授、博士生导师, 主要研究方向为数值优化、图像处理、数据安全。