计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2024,33(1):272−279 [doi: 10.15888/j.cnki.csa.009354]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

基于动态加权选举的委托权益证明共识机制改进①

杨　攀, 苏　波, 刘敏贤, 叶传涛, 胡谊玲, 张　伟

(西南科技大学 计算机科学与技术学院, 绵阳 621010)
通信作者: 苏　波, E-mail: bosu@foxmail.com

摘　要: 面向委托权益证明共识机制中用户节点缺乏积极性、节点窜谋、难以抑制恶意节点出现、中心化风险变高等缺陷, 提出了一种基于动态加权选举的委托权益证明共识机制改进方案. 首先, 针对用户节点建立奖惩机制以激励用户参与选举活动, 同时引入用户节点地址聚类算法以发现具有相似投票行为的用户节点, 限制用户节点的不良投票行为. 使用改进熵权法对每一轮候选节点的特征动态计算权值, 再利用优劣解距离算法结合用户节点的投票情况对候选节点进行排序, 使选举结果更为合理. 随后, 在区块生产过程中动态调整生产节点的生产顺序以避免中心化风险. 最终通过仿真模拟验证了所提改进方案的可行性与有效性, 结果表明, 所提方案能在激励用户节点的同时限制节点的不良行为, 有效降低恶意节点出现的概率并避免中心化风险.

关键词: 区块链; 委托权益证明; 共识机制; 动态加权选举

引用格式: 杨攀,苏波,刘敏贤,叶传涛,胡谊玲,张伟.基于动态加权选举的委托权益证明共识机制改进.计算机系统应用,2024,33(1):272–279. http://www.c-s-a.org.cn/1003-3254/9354.html

Improvement of Consensus Mechanism of Delegated Proof of Stake Based on Dynamic Weighted Election

YANG Pan, SU Bo, LIU Min-Xian, YE Chuan-Tao, HU Yi-Ling, ZHANG Wei

(School of Computer Science & Technology, Southwest University of Science and Technology, Mianyang 621010, China)

Abstract: This study presents a proposal to improve the delegated proof of stake consensus mechanism based on dynamic weighted election, so as to mitigate issues such as the lack of initiative in user nodes, collusion among nodes, difficulty in suppressing malicious node appearance, and increased centralization risk. Firstly, a system of rewards and penalties is established for user nodes to incentivize users' participation in the election process. Moreover, an address clustering algorithm of user nodes is introduced to identify user nodes exhibiting similar voting behavior, effectively curbing undesirable voting actions of user nodes. The enhanced entropy weighting method is utilized to dynamically calculate the weights of each candidate node's features during each round of the election process. The voting results of user nodes are combined with the performance distance algorithm to rank the candidate node, leading to more rational election results. Subsequently, in the block production process, the production order of production nodes is dynamically adjusted to avoid the centralization risk. Finally, the feasibility and effectiveness of the proposed scheme are validated through simulation. The results demonstrate that the proposed scheme can not only incentivize user nodes but also limit the bad behavior of nodes, effectively reducing the probability of malicious nodes and avoiding centralization risk.

Key words: blockchain; delegated proof of stake (DPoS); consensus mechanism; dynamic weighted election

① 基金项目: 西南科技大学博士基金 (19zx7142)
收稿时间: 2023-06-01; 修改时间: 2023-07-12, 2023-08-08; 采用时间: 2023-08-11; csa 在线出版时间: 2023-11-24
CNKI 网络首发时间: 2023-11-27

自以加密货币为代表的区块链应用首次诞生以来, 作为技术基础的区块链就备受公众关注. 区块链系统具备不可篡改、透明、可溯源等特性[1], 在金融、能源、供应链管理等领域具有广泛的应用前景[2]. 区块链技术作为一种创新型的技术架构, 其核心技术包括对等网络、默克尔树、非对称加密、智能合约、共识机制等[3], 其中, 共识机制是任何区块链系统中的一个重要组成部分, 其用于保障区块链网络中对等节点之间数据的完整性与有效性, 并且维护着区块链网络节点的稳定, 因此, 共识机制在很大程度上决定了区块链系统的性能与安全[4]. 由于区块链系统面临着“不可能三角”问题[5], 即安全、吞吐性能、去中心化程度 3 方面无法同时达到最好的状态, 因此研究人员针对不同应用领域的特点与使用需求设计了不同的共识机制. 当前区块链公有链系统中主流的共识机制包括工作量证明 (proof of work, PoW)、权益证明 (proof of stake, PoS) 与委托权益证明 (delegated proof of stake, DPoS), 以比特币为代表的基于 PoW 的区块链系统都存在着性能方面的缺陷, 且需要消耗大量的能源以维持区块链系统的稳定运行[6]. 为了解决 PoW 在达成共识过程中的算力浪费问题, 研究人员提出了 PoS 共识机制, 使用权益证明的方式取代了基于算力竞争的工作量证明来决定记账权的归属, 解决了算力浪费的问题, 但当区块链网络发展到一定程度时, 容易出现马太效应, 即权力越来越集中在少数人手中, 加大了区块链系统中心化的风险[7]. DPoS 共识机制在 PoS 的基础上引入了投票选举机制, 以牺牲部分去中心化程度的方式实现了较高的交易吞吐量, 并在一定程度上解决了算力浪费与马太效应的问题, 更适用于大规模的应用场景, 被视为区块链 3.0 的代表[8]. 在基于 DPoS 共识机制的区块链系统中, 并非所有对等节点都可参与共识过程, 区块链系统中交易的验证与区块的打包活动仅由部分被选中的节点负责, 其选举流程大致如图 1 所示, 满足一定硬件条件的节点即可参与竞选成为候选节点, 在理想状况下, 候选节点会通过为区块链社区做出贡献以拉取选票, 普通用户节点将选票投给候选节点, 最终将各个候选节点按照得票数进行排序, 以固定数量选出排名靠前的节点, 当选的这部分节点被称为生产节点, 其余未成功当选节点则作为备用节点仅同步区块链系统中的链上数据, 不参与共识过程.

然而, 这种独特的选举机制为区块链系统引入了如下新的风险.

(1) 由于生产者节点仅由选举活动产生, 但当前机制中的选举活动对于用户的投票行为没有任何限制, 并且缺乏对于候选节点的评价机制, 因此选举活动不能及时有效地阻止恶意节点或不合格的节点当选为生产者节点, 进而影响区块链系统的稳定性[9].

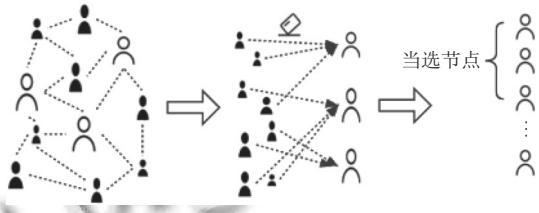

图 1 DPoS 共识机制选举流程

(2) 选举结果与最终获利密切相关, 因此在选举过程中容易出现各个利益团体相互勾结的现象, 损害普通用户节点的利益, 且普通用户节点无法直接从选举中获利, 所以用户的投票参与率普遍不高[10].

(3) 由于记账节点的减少使得区块链系统的区块生产权力容易被少部分节点所掌控, 增加了系统的中心化风险, 区块的有效性与数据的完整性将难以得到保证.

上述缺陷制约着基于 DPoS 共识机制的区块链系统得到更广泛地应用, 因此, 共识机制的优化与改进工作对于推动区块链技术的发展和应用具有重要意义. 本文针对上述缺陷, 从节点动态评价、用户投票行为与去中心化程度限制 3 个方面考虑, 提出了一种基于动态加权选举的委托权益证明共识机制改进方案. 该方案基于生产者节点与用户在每轮共识过程中的行为进行动态评价, 鉴别出具有异常行为的生产者节点与用户, 组合选举出合理的节点参与区块生产, 通过附加机制以抑制上述风险.

本文在后续的相关研究章节阐述了对于 DPoS 共识机制改进的侧重点. 在共识机制改进方案章节中, 详细描述了本文提出的方法, 并在实验分析章节中进行了对比分析. 结果表明, 本文所提方法在提升上述缺陷方面具有显著效果.

1 相关研究

当前, 大部分针对 DPoS 共识机制的改进工作大都针对某一方面的具体缺陷引入附加机制以提升区块链系统在该方面的表现. 底层硬件的改进方面, Bao 等[11]探讨了将因特尔软件保护扩展 (Intel software

guard extensions, Intel SGX) 技术应用于区块链领域, 从硬件层面提升区块链系统的安全性. DPoS 共识机制中的生产者节点由选举过程产生, 因此选举制度是否设置合理对于区块链系统的正常运行至关重要. 为加快剔除生产者节点队列中出现的恶意节点与不合格节点, 文献[12]在生产者节点的选举环节中引入了熔断机制, 新增了投反对票的选项. 文献[13]将投票选项具体到了赞同、非常赞同、反对与非常反对这 4 项, 使投票结果能更准确地反映用户的期望. 传统 DPoS 共识机制的选举过程并不能阻止恶意节点与不合格节点的出现, 针对此项缺陷不少研究人员从加权投票的角度入手, 依托不同的权重计算最终得票数, 使选举结果更为合理可信. 文献[14]建立了节点活跃度的量化方法, 基于节点的活跃度与加权投票的组合分析选举出合适的生产者节点. 文献[15]提出了节点信誉值概念, 节点的负向行为将会受到信誉值降低的惩罚, 选举结果由节点的得票数与自身信誉值共同决定. 文献[16]针对节点建立了信誉度模型, 并提出了基于投票和信誉度的组合评估方案以提高生产者节点的可靠性. 面对普通用户节点投票不积极、选举进展缓慢等缺陷, 文献[17]引入了奖励制度, 其提出的奖励制度包含了投票奖励与举报奖励两大类, 其中投票奖励用于激励节点积极参与投票活动, 举报奖励用于激励用户节点举报有不良行为的节点. 文献[18]建立了一个聚类模型以对用户节点进行聚类分析, 并根据聚类结果对不同类型的用户节点进行奖励, 从而提高用户节点投票的积极性.

总体来说, 当前对于 DPoS 共识机制的改进主要集中在对于其选举过程的改进, 通过多因素加权评估使选举结果更为合理, 但对于加权评估而建立的组合分析模型大都为静态模型, 并采用主观赋权的方式对模型中的指标进行赋权, 缺乏对于节点在不同时序特征的动态分析, 且仅从被选举者的角度考虑, 缺乏对选举者的行为进行限制. 本文在上述研究的基础上提出了基于动态加权组合选举的 DPoS 共识机制 (DPoS based on dynamic weighted election, DPoSDWE), 本文所提的改进方案中首先选取节点的特征项, 基于节点的特征历史数据动态分析各特征项的权重, 同时对于用户节点引入奖惩机制以限制用户节点的行为并激励用户节点参与选举活动, 根据用户节点的投票行为建立用户节点地址聚类模型, 将拥有相似投票行为的用户节点地址视为同一个实体, 其投票权重将会被加以限制, 将节点的与用户节点的投票权重结合, 从选举者与被选举者两个角度组合分析得出最终的选举结果, 择优选取生产者节点. 同时以限制中心化程度为目的针对区块链中心化程度动态调控区块链系统的区块生产活动, 避免了中心化风险.

2 DPoS 共识机制改进方案

本文所提改进方案主要改进了生产者节点的选举过程和区块生产过程. 在选举过程中, 首先计算候选节点特征项的权值, 然后对用户节点地址进行聚类, 根据聚类结果限制用户的投票行为, 最后根据候选节点的特征项和得票数来选择参与共识的节点. 而在区块生产过程中, 则通过不断调整生产者节点的出块顺序来限制中心化程度.

2.1 候选节点特征权值计算

合理地确定对等节点各个特征项的权重对于后续评价节点历史表现至关重要. 对等节点在参与区块链系统的共识过程、维持区块链系统的正常运行中产生了大量的历史数据, 如表征节点性能的 CPU 与网络占用率等信息, 该部分数据为评价节点的表现提供了参考价值. 熵权法是一种常用的权重计算方法, 其核心思想为某一项指标的数据离散程度越大, 则所蕴含的信息越多, 该指标的权重也就越大, 避免了主观因素带来的影响, 但传统的熵权法在面对特征熵值趋近于零时容易出现失真的情况[19], 而本文研究对象的部分指标可能存在着特征熵值过多的情况, 因此本文采用一种经过改进的熵权法计算权重, 其既能克服传统熵权法中的缺陷, 又能保持拉开各个指标之间差距的能力[20].

首先, 按照式 (1) 对负向指标进行正向化处理:

$$x'_{ij}=\frac{\max\left\{x_{ij},\cdots,x_{nj}\right\}-x_{ij}}{\max\left\{x_{ij},\cdots,x_{nj}\right\}-\min\left\{x_{ij},\cdots,x_{nj}\right\}} \tag{1}$$

其中, x_{ij}表示第i个样本的第j个特征指标, x'_{ij}表示归一化的数值.

再按照式 (2) 对数据进行标准化处理:

$$z_{ij}=x_{ij}\Big/\sqrt{\sum_{i=1}^{n}x_{ij}^2} \tag{2}$$

完成数据标准化后, 按照式 (3) 计算每个指标的熵值:

$$E_j = -\frac{1}{\ln n}\sum_{i=1}^{n}\frac{z_{ij}}{\sum_{i=1}^{n} z_{ij}}\ln\frac{z_{ij}}{\sum_{i=1}^{n} z_{ij}} \tag{3}$$

改进的权重计算部分如下:

$$\omega_j = \begin{cases} \left(1-\bar{E}^{35.35}\right)\omega_{0j} + \bar{E}^{35.35}\omega_{3j}, & E_j < 1 \\ 0, & E_j = 1 \end{cases} \tag{4}$$

$$\omega_{0j} = \frac{1-E_j}{\sum_{j=1}^{n}\left(1-E_j\right)} \tag{5}$$

$$\omega_{3j} = \frac{1+\bar{E}-E_j}{\sum_{k=1,E_k\neq 1}^{n}\left(1+\bar{E}-E_k\right)} \tag{6}$$

其中, $\bar{E}$ 表示所有熵值不等于 1 的平均值, ω_j 即为第 j 个指标的权重.

改进熵权法与传统熵权法的结果对比如表 1 所示.

表 1 改进前后熵权法效果对比

方法	熵值	权值
传统熵权法	[0.999 1, 0.999 0, 0.999 2]	[0.333, 0.370, 0.296]
改进熵权法	[0.999 1, 0.999 0, 0.999 2]	[0.333, 0.336, 0.332]

当特征项熵值趋向于零且差异较小时, 使用传统的熵权法计算得出的权值会出现较大的差距, 而使用改进后的熵权法计算得出的权值更为合理.

2.2 用户节点地址聚类算法

尽管公有链系统中每个用户节点的行为记录都公开可查询, 但由于其匿名的特性导致难以确定用户节点的真实信息, 因此在传统 DPoS 共识机制的选举过程中, 存在着利益相关者相互勾结操纵选举、节点腐败等不良现象, 损害了普通用户节点的利益. 为了及时发现选举过程中出现的异常现象、限制不良行为, 本文引入了用户节点地址聚类算法以发现潜在的受同一实体控制或具有共同利益目的用户地址, 算法步骤如算法 1 所示.

算法 1. 用户地址聚类算法

输入: 投票用户地址集 V, 相似度测量函数 Sim, 相似度阈值 θ.
输出: 具有相似投票行为的用户地址集 C.

1) $C = \varnothing$ //初始化相似投票行为用户地址簇
2) $checked = \varnothing$ /初始化以检查用户地址集
3) **for** v_p **in** $\{voters \mid voters \in V, voters \notin checked\}$ **do**
4) $checked$.**append** (v_p)
5) $C_t = \varnothing$ //创建临时用户地址簇
6) C_t.**append** (v_p)
7) **for** v_a **in** $\{voters \mid voters \in V, voters \notin checked\}$ **do**
8) **if** $Sim(v_p, v_a) < \theta$ **then**
9) $checked$.**append** (v_a)
10) C_t.**append** (v_a)
11) **if** C_t.**length** > 1 **then**
12) C.**append** (C_t)

本文中相似度测量函数使用 Jaccard 系数[21], 计算 u、v 两个用户投票行为相似的方法如式 (7) 所示:

$$Sim(u,v) = \sum_{i=1}^{n}\frac{|R_i(u)\cap R_i(v)|}{|R_i(u)\cup R_i(v)|} \tag{7}$$

其中, n 表示两用户共同参与的投票次数, R_i 表示用户在该次投票的行为记录. 由于基于投票活动的用户行为不可避免的具有相似性, 故本文设置了相似度阈值, 当量化后的相似度超出相似度阈值后才将用户投票行为归结为异常行为.

2.3 用户节点行为限制机制

当前的 DPoS 共识机制中由于普通用户节点无法直接从投票选举中获利, 进而存在着用户节点参与度不高、选举过程进展缓慢的问题. 以基于 DPoS 共识机制的 EOSIO 区块链系统为例, 其在运行初期选举过程中的用户参与率不足 5%[22]. 合理的奖惩机制可吸引更多的用户节点参与投票, 并可及时阻止节点窜谋选举等异常投票行为.

为了限制用户节点投票的不良行为, 本文引入了投票权重, 每个用户节点的投票权重与各自节点的行为直接相关, 投票权重的计算方法如下:

$$weight_{jv} = \begin{cases} 1-sim_v, & v \in C \\ 1, & v \notin C \end{cases} \tag{8}$$

其中, $weight_{jv}$ 表示用户节点 对目标候选节点 的投票权重, $v \in C$ 表示该用户节点隶属于地址聚类中的一个簇, sim_v 表示用户节点 v 与簇中其他用户节点的最大 Jaccard 相似度. 用户节点的投票权重根据用户的投票行为与历史不断积累, 限制了用户节点的不良投票行为, 降低了节点窜谋的可能性.

同时, 本文引入了用户节点投票收益, 对于每一个参与了投票的用户节点系统会发放奖励, 奖励即为用户节点的投票收益, 投票收益的定义如下:

$$reward_v = \sum_{i=1}^{n}\sum_{j=1}^{t} weight_{jv} \times m/8 \tag{9}$$

其中, n 表示用户 v 参与的投票中投向正常节点的总次

数, t表示本轮投票中用户v投向目标候选节点的数量, m表示本轮投票中总参与人数. 用户投票收益可使用户节点直接从参与投票中获益, 激励用户参与投票过程, 增加了社区的活跃度.

2.4 改进方案

为使选举结果更加公正合理且为尽量避免恶意节点当选, 本文提出的选举改进方案从候选节点的历史表现和用户的投票行为两方面综合评估节点, 择优选出固定数量的生产者节点, 选举流程如图 2 所示.

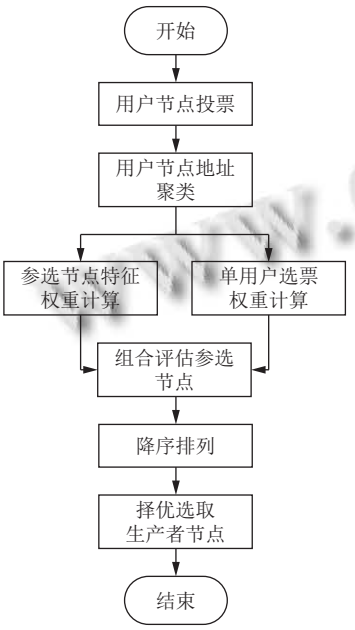

图 2 改进选举流程

当前的 DPoS 共识机制中对于用户节点的投票行为没有任何限制措施, 用户节点可将持有的代币置换为选票投给候选节点, 持币量大的用户节点对选举结果的影响也较大, 因此存在着选举过程被操纵的隐患. 在本文提出的改进方案中, 将每个用户实际投出的选票数量根据用户的投票行为重新计算, 最终得出目标候选节点的实际得票数, 目标候选节点实际得票数的计算方法如下所示:

$$votes_{jv} = weight_{jv} \times voter_{vj} \tag{10}$$

其中, $voter_{vj}$为用户节点v对候选节点j的实际投票数, 为候选者节点$votes_{jv}$的最终从用户节点j获得的票数.

之后根据候选节点的行为特征与最终得票数对候选节点进行排序. 本文选取两轮选举之间的节点特征指标数据为样本, 以节点 CPU 与网络占用率、节点打包区块数量、节点超时未提交区块次数、节点账户余额、节点最终得票数为指标按照第 2.1 节所述方法计算权重.

候选节点排序方法如下, 对于已经正向标准后的特征矩阵分别定义候选节点中的最优评价与最劣评价.

$$Z^{+} = (\max\{z_{11}, z_{21}, \cdots\}, \cdots, \max\{z_{1m}, z_{2m}, \cdots\}) \tag{11}$$

$$Z^{-} = (\min\{z_{11}, z_{21}, \cdots\}, \cdots, \min\{z_{1m}, z_{2m}, \cdots\}) \tag{12}$$

其中, Z^{+}表示最优评价, Z^{-}表示最劣评价. 分别按式 (13) 与式 (14) 计算候选节点与最优评价和最劣评价之间的欧氏距离.

$$D_i^{+} = \sqrt{\sum_{j=1}^{m} \omega_j \left(Z_j^{+} - z_{ij}\right)^2} \tag{13}$$

$$D_i^{-} = \sqrt{\sum_{j=1}^{m} \omega_j \left(Z_j^{-} - z_{ij}\right)^2} \tag{14}$$

其中, ω_j为第j个指标的权重, 按照式 (15) 计算候选节点的综合评估分数.

$$S_i = \frac{D_i^{-}}{D_i^{+} + D_i^{-}} \tag{15}$$

其中, S_i表示第i个候选节点的最终得分, 将候选节点按照最终得分降序排列后选择排行靠前的节点作为生产者节点参与共识.

去中心化作为区块链系统的核心功能之一, 为实现解决信任问题、降低互信成本的区块链本质目的提供了技术支撑, 因此去中心化程度对于区块链系统的数据完整性和用户信任度至关重要. 在 DPoS 共识机制中生产者节点之间采用协作而非竞争的方式生产区块, 每一轮生产周期中生产者节点按照固定的生产顺序轮流生产一定数量的区块, 若某个节点未在限定时间内提交区块, 则在本次生产周期内跳过该节点, 该机制可能会使部分节点在区块生产过程中占据过多权重, 使区块链系统区块生产过程的去中心化程度降低. 以往研究中使用信息熵度量区块链系统的去中心化程度[23], 本文同样引入信息熵的概念以量化区块链系统区块生产过程的去中心化程度.

$$p_j = \frac{b_j}{\sum_{j=1}^{n} b_j} \tag{16}$$

$$D_i = -\sum_{j=1}^{n} p_j \log_2 p_j \tag{17}$$

其中, D_i表示第i轮生产周期中的去中心化程度, n表示生产者节点的数量, b_j表示第j个生产者节点在本轮生产周期中提交的区块数. 为限制生产过程中的中心化程度, 本文不再固定生产者节点提交区块的顺序, 而是通过计算节点适宜值动态地从生产者节点列表中选取适宜值最高的节点负责打包区块, 计算方法如下:

$$A_j = \frac{1-p_j}{e^{o_j}} \tag{18}$$

其中, o_j表示表示生产者节点j当前生产周期内超时未提交区块的次数, A_j为节点j当前的适应值. 单次区块生产的流程如图 3 所示.

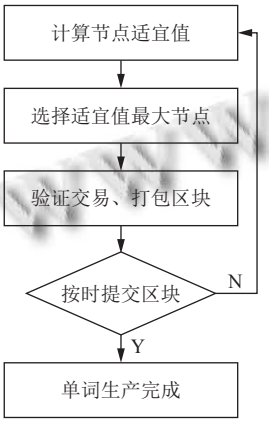

图 3 单次区块生产流程

3 实验分析

为了检验本文所提共识机制改进方案的有效性, 在相同的实验环境下对 DPoS 共识机制改进前后的表现进行了对比分析, 实验设定在单台计算机上进行仿真模拟, 操作系统为 macOS 12.3.1, CPU 平台为 i5-7500 HQ, 24 GB 内存.

3.1 用户参与度

改进方案中引入的奖惩机制主要用户激励用户节点参与投票活动并限制用户节点的不良投票行为. 为验证本文所提改进方案中引入的奖惩机制的激励作用, 本文分别在改进前后的 DPoS 共识机制中创建相同数量的用户节点进行模拟投票, 其中在用户节点中都设置了 10% 的持有大量选票的用户节点, 即此类用户对于选举结果有较大的影响, 无需激励制度也能表现出较强的投票意愿, 且部分用户节点会由于共同的利益目标投向相同的候选节点. 仿真测试中共进行了 100 轮模拟投票, 结果如图 4 所示.

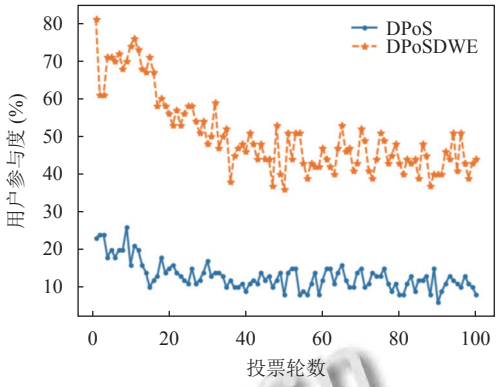

图 4 用户参与度对比

改进前后的 DPoS 共识机制中, 用户节点的参与度在投票的初始阶段都处于各自的较高水平, 改进前的共识机制中用户节点的参与度经过 20 轮投票过后最终占比在 10% 左右徘徊, 即实验中设置的持有大额选票的用户节点的比例. 而在改进后的共识机制中, 用户的参与度有了明显的提升, 即使是在后期阶段也有 40%−50% 的用户节点参与投票活动, 表明了改进方案中引入的奖惩机制能有效地激励用户节点.

3.2 相似投票行为用户占比

本文引入了用户地址聚类模型以发现具有相似投票行为的用户节点, 为验证奖惩机制对于用户节点不良投票行为的限制作用, 本文在改进前后的共识机制中分别对比了参与投票的用户中具有相似投票行为的用户节点占比, 该部分测试于第 4.1 节同步进行, 地址聚类模型中相似度阈值设定为 0.8, 对比结果如图 5 所示.

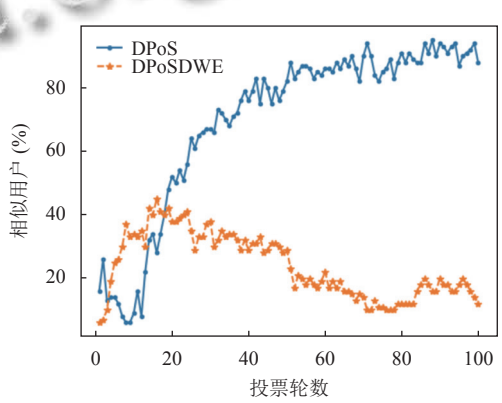

图 5 相似行为用户占比

改进前的 DPoS 共识机制中, 20 轮投票过后具有相似投票行为的比例迅速升高, 达到了 80% 以上, 结合第 3.1 节中的测试结果分析, 20 轮投票过后大部分普通用户节点以丧失了参与投票的意愿, 而余下的持

有大额选票的用户节点因为共同的利益目标大部分都具有相似的投票行为. 改进后的 DPoS 共识机制中, 相似用户的比例在投票前期短暂的上升后呈现出了下降的趋势, 验证了奖惩机制在抑制用户节点不良投票行为方面的有效性.

3.3 恶意节点占比

为检验改进的选举过程是否能有效地避免恶意节点的出现, 本文在模拟共识过程的初期阶段中为生产节点中加入了 25% 的恶意节点, 结果如图 6 所示.

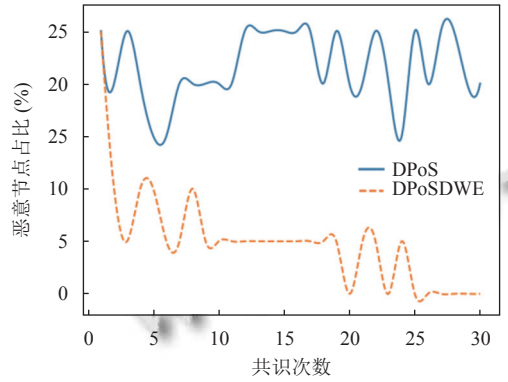

图 6 恶意节点比例变化

随着共识次数的增加, 改进前的 DPoS 共识机制中恶意节点在生产节点中的比例并未出现明显下降的趋势. 而改进后的 DPoS 共识机制中恶意节点占比随着共识次数的增加而呈现出了下降的趋势, 在仿真模拟中最终趋向于 0, 改进后的 DPoS 共识机制可有效地阻止恶意节点当选.

3.4 去中心化程度

仿真实验中还设置了 DPoS 共识机制改进前后系统的去中心化程度对比以检验动态调整节点生产顺序机制的有效性, 去中心化程度的量化方法如第 2.4 节所述, 测试结果如图 7 所示.

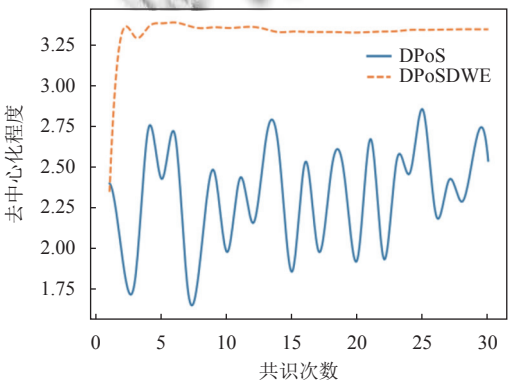

图 7 去中心化程度对比

由图 7 可知, 在改进前的 DPoS 共识机制中, 区块链系统生产过程的去中心化程度量化分随着共识次数的增多而波动, 并未呈现出明显的变化趋势. 改进后的 DPoS 共识机制中, 区块链系统生产过程的去中心化程度经历了初始的上升阶段后一直保持在一个稳定的水平, 且所有阶段均高于未改进前的去中心化程度.

3.5 与现有改进方案对比

本节中总结了本文所提的改进方案与现有改进方案的差异, 比较结果如表 2 所示.

表 2 改进方案对比

改进方案	抑制恶意节点	激励用户节点	限制节点行为	限制中心化
文献[12,13]	√	—	—	—
文献[14]	√	√	√	—
文献[15,16]	√	—	√	—
文献[17,18]	—	√	—	—
本文方案	√	√	√	√

与现有的代表性改进方案进行对比, 可以看出本文所提的改进方案考虑的方面更多, 能够从抑制恶意节点、激励用户节点、限制节点行为、限制中心化 4 个角度进行改进, 帮助提升区块链系统的表现.

4 结语

共识机制是决定区块链系统安全与性能的最关键因素, 本文针对 DPoS 共识机制中选举机制不能阻止恶意节点、用户节点参与度过低、不能限制用户节点行为、存在中心化风险等缺陷, 提出了基于加权动态组合选举的共识机制改进方案, 并通过仿真实验验证了所提方案的可行性与有效性. 未来工作将集中于优化模型细节, 提高共识机制的效率, 并挖掘共识机制的应用场景, 将该共识机制与实际应用相结合.

参考文献

1 代闯闯, 栾海晶, 杨雪莹, 等. 区块链技术研究综述. 计算机科学, 2021, 48(S2): 500–508.

2 Abou Jaoude J, Saade RG. Blockchain applications-usage in different domains. IEEE Access, 2019, 7: 45360–45381. [doi: 10.1109/ACCESS.2019.2902501]

3 Zheng ZB, Xie SA, Dai HN, *et al*. An overview of blockchain technology: Architecture, consensus, and future trends. Proceedings of the 2017 IEEE International Congress on Big Data. Honolulu: IEEE, 2017. 557–564.

4 Lashkari B, Musilek P. A comprehensive review of

blockchain consensus mechanisms. IEEE Access, 2021, 9: 43620–43652. [doi: 10.1109/ACCESS.2021.3065880]
5 靳世雄, 张潇丹, 葛敬国, 等. 区块链共识算法研究综述. 信息安全学报, 2021, 6(2): 85–100.
6 Kohli V, Chakravarty S, Chamola V, *et al*. An analysis of energy consumption and carbon footprints of cryptocurrencies and possible solutions. Digital Communications and Networks, 2023, 9(1): 79–89. [doi: 10.1016/j.dcan.2022.06.017]
7 Nguyen CT, Hoang DT, Nguyen DN, *et al*. Proof-of-stake consensus mechanisms for future blockchain networks: Fundamentals, applications and opportunities. IEEE Access, 2019, 7: 85727–85745. [doi: 10.1109/ACCESS.2019.2925010]
8 Zhang CQ, Wu CS, Wang XY. Overview of Blockchain consensus mechanism. Proceedings of the 2nd International Conference on Big Data Engineering. Shanghai: ACM, 2020. 7–12.
9 Sharma M, Pant S, Kumar Sharma D, *et al*. Enabling security for the industrial Internet of Things using deep learning, blockchain, and coalitions. Transactions on Emerging Telecommunications Technologies, 2021, 32(7): e4137. [doi: 10.1002/ett.4137]
10 刘艺华, 陈康. 区块链共识机制新进展. 计算机应用研究, 2020, 37(S2): 6–11.
11 Bao ZJ, Wang QH, Shi WB, *et al*. When blockchain meets SGX: An overview, challenges, and open issues. IEEE Access, 2020, 8: 170404–170420. [doi: 10.1109/ACCESS.2020.3024254]
12 黄嘉成, 许新华, 王世纯. 委托权益证明共识机制的改进方案. 计算机应用, 2019, 39(7): 2162–2167.
13 Liu J, Xie MY, Chen SY, *et al*. An improved DPoS consensus mechanism in blockchain based on PLTS for the smart autonomous multi-robot system. Information Sciences, 2021, 575: 528–541. [doi: 10.1016/j.ins.2021.06.046]
14 Wang B, Li HL, Pan L. Optimized DPoS consensus strategy: Credit-weighted comprehensive election. Ain Shams Engineering Journal, 2023, 14(2): 101874. [doi: 10.1016/j.asej.2022.101874]
15 任南, 马园园. DPoS 共识机制改进的演化博弈及策略研究. 计算机工程与应用, 2022, 58(12): 102–111.
16 Sun YY, Yan BW, Yao Y, *et al*. DT-DPoS: A delegated proof of stake consensus algorithm with dynamic trust. Procedia Computer Science, 2021, 187: 371–376. [doi: 10.1016/j.procs.2021.04.113]
17 陈梦蓉, 林英, 兰微, 等. 基于“奖励制度”的 DPoS 共识机制改进. 计算机科学, 2020, 47(2): 269–275.
18 Wang LJ, Xu PH, Su W, *et al*. Research on improvement of blockchain DPOS consensus mechanism based on HK clustering. Proceedings of the 2021 China Automation Congress. Beijing: IEEE, 2021. 1167–1172.
19 Zhu YX, Tian DZ, Yan F. Effectiveness of entropy weight method in decision-making. Mathematical Problems in Engineering, 2020, 2020: 3564835.
20 欧阳森, 刘丽媛. 配电网用电可靠性指标体系及综合评估方法. 电网技术, 2017, 41(1): 222–229.
21 Bag S, Kumar SK, Tiwari MK. An efficient recommendation generation using relevant Jaccard similarity. Information Sciences, 2019, 483: 53–64. [doi: 10.1016/j.ins.2019.01.023]
22 Zheng WL, Zheng ZB, Dai HN, *et al*. XBlock-EOS: Extracting and exploring blockchain data from EOSIO. Information Processing & Management, 2021, 58(3): 102477.
23 Liu JL, Zheng WL, Lu DY, *et al*. From decentralization to oligopoly: A data-driven analysis of decentralization evolution and voting behaviors on EOSIO. IEEE Transactions on Computational Social Systems, 2023, 10(5): 2752–2763. [doi: 10.1109/TCSS.2022.3191350]

(校对责编: 孙君艳)