doi:10.14132/j.cnki.1673-5439.2025.05.010

区块链中基于多级委员会的去中心化节点管理方法

胡筱旋[1],喻天豪[1],董振江[2],孙雁飞[1],温 砚[3],亓 晋[1]

(1. 南京邮电大学 物联网学院,江苏 南京 210003
2. 南京邮电大学 计算机学院,江苏 南京 210023
3. 江苏智檬智能科技有限公司,江苏 南京 210046)

摘要:针对基于委员会的区块链系统存在中心化程度高、节点投票积极性低、易被操纵等问题,提出一种基于多级委员会的去中心化节点管理方法。该方法引入节点综合评估模型对全网节点进行初步筛选,并设计积分衰退算法动态选举出块节点,保障系统的去中心化特性,最后引入奖惩激励机制促进节点在区块链系统中保持积极行为。实验表明,提出的多级架构与共识算法相较同类算法提高了区块链系统的去中心化水平,并在抗操纵能力、出块速度、节点投票积极性和恶意节点剔除速度等方面性能更佳。

关键词:区块链;权益委托证明;多级委员会;积分衰退

中图分类号:TP311 **文献标志码**:A **文章编号**:1673-5439(2025)05-0085-09

A decentralized node management approach based on multi-level committees in blockchains

HU Xiaoxuan[1], YU Tianhao[1], DONG Zhenjiang[2], SUN Yanfei[1], WEN Yan[3], QI Jin[1]

(1. College of Internet of Things, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
2. School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China
3. Jiangsu Zhimeng Intelligent Technology Co., Ltd., Nanjing 210046, China)

Abstract: In response to the challenges of high centralization, low node voting enthusiasm, and vulnerability to manipulation in committee-based blockchain systems, this paper proposes a decentralized node management method based on a multi-level committee structure. The method introduces a comprehensive node assessment model for preliminary screening of all network nodes, and incorporates a point decay algorithm to dynamically elect block-producing nodes, thereby ensuring the system's decentralized nature. Finally, a reward and punishment incentive mechanism is introduced to encourage nodes to maintain active behavior within the blockchain system. Experiments show that the multi-level architecture and the proposed consensus algorithm improve the decentralization level of the blockchain system compared to similar algorithms, and achieve better performance in terms of resistance to manipulation, block production speed, node voting enthusiasm, and the speed of malicious node removal.

Keywords: blockchain; delegated proof of stake; multi-level committees; scoring decay

收稿日期:2024-09-17;**修回日期**:2025-02-18 **本刊网址**:http://nyzr.njupt.edu.cn

基金项目:江苏省重点研发计划重点项目(BE2023025, BE2023025-1, BE2023025-4)、江苏省高等学校基础科学(自然科学)研究项目(22KJB520028)和南京邮电大学引进人才自然科学研究启动基金(NY221146)资助项目

作者简介:胡筱旋,女,博士,讲师;亓晋(通信作者),男,博士,教授,qijin@njupt.edu.cn

引用本文:胡筱旋,喻天豪,董振江,等.区块链中基于多级委员会的去中心化节点管理方法[J].南京邮电大学学报(自然科学版),2025,45(5):85-93.

Citation: HU Xiaoxuan, YU Tianhao, DONG Zhenjiang, et al. A decentralized node management approach based on multi-level committees in blockchains[J]. Journal of Nanjing University of Posts and Telecommunications(Natural Science Edition), 2025, 45(5): 85-93.

区块链技术以其不可篡改性、保证数据完整性、可追溯性等特点[1-2],在金融科技、物联网等多个领域迅速发展[3]。其中,共识机制是区块链的核心技术,网络节点可以通过共识机制制定的规则,进行区块有效性验证以及生产下一区块[4]。目前联盟链[5]中常用的共识机制为实用拜占庭容错(Practical Byzantine Fault Tolerance, PBFT)[6],主流的公有链[7]共识机制有工作量证明(Proof of Work, PoW)[8]和股权证明(Proof of Stake, PoS)[9]。然而,传统共识在交易处理吞吐量上存在瓶颈,因此2014年Larimer[10]设计并提出了委托权益证明(Delegated Proof of Stake, DPoS)来提高区块链系统的交易验证速度。

在DPoS机制中,持币用户通过抵押代币获得选票,以投票的方式选出若干的节点作为区块生产者轮流生成区块,并负责验证交易。在每轮共识中,所有代币持有者可以将投票权委托给信任的节点候选人,选出新的见证人参与共识。相比PoS,DPoS减少了直接参与共识的节点数量,以一定程度的中心化为代价,极大提升了区块确认速度至秒级[11],且能够降低能耗,进一步提高了区块链系统性能。作为最主要的共识算法之一,DPoS已经在BitShares、Steem、EoS(Enterprise Operation System,企业级操作系统)等项目上获得了广泛的应用,但仍存在着中心化程度高、投票积极性低、易遭受恶意攻击等缺点[12]。

针对以上问题,近年来许多学者在如何提升区块链系统性能上进行了改进。Li等[13]提出了一种基于GN算法的节点投票热情测量方法,并通过设计节点信用激励机制,激励正常节点投票。侯凯祥等[14]通过预验证机制在较小开销的前提下对委员会进行可靠的信誉评估,及时淘汰委员会中的恶意节点。Xu等[15]提出使用模糊集投票方法来降低节点共谋投票的可能性。付晓东等[16]借鉴博弈理论中权力指数的思想,构建DPoS的加权投票博弈模型,提出基于权力指数的DPoS共谋攻击检测与预防方法。然而,上述方案仍存在共识机制中心化程度高和节点垄断的问题。

为了解决以上问题,Tan等[17]提出利用Borda Count来选择更符合其他节点意愿的节点,提高选举的公平性。You等[18]提出了热衰减机制对那些长期保持高排名的节点进行温和惩罚,减少了巨量垄断现象,增强了全网的去中心化程度,但仍没有摆脱股权投票带来的公平性问题。

综上所述,目前对于DPoS共识机制的改进主要集中于对于网络节点竞选见证节点的选举过程,将研究点放在提高共识速度和委员会节点可靠性上[14],忽略了见证节点垄断的问题,导致区块链系统去中心化程度降低。现有的针对去中心化问题的解决方案无法很好地兼顾选举公平性与节点垄断问题[19],并且缺少对区块链网络安全性和节点投票积极性的综合考量。

因此,本文提出一种区块链中基于多级委员会的去中心化节点管理方法。该方法为公有链区块链系统设计了一种新的节点框架结构,并通过设计MC-DPoS共识算法优化了区块生产与验证中节点的选拔与分工过程。该方法可以良好适配诸多以区块链技术为基础的应用领域,为自主交易、供应链等需求场景提供更民主的去中心化平台。本文的工作总结如下:

(1)提出了区块链中基于多级委员会的去中心化节点管理方法,设计区块链多级委员会架构,可以将区块链区块生产验证流程进行模块化处理,并分级处理网络节点。

(2)基于多级委员会架构设计了动态共识算法MC-DPoS,设计次级委员会选举算法、积分衰退算法、可验证随机函数抽签算法实现网络节点的升降级机制,动态分配节点在区块链系统中的角色定位。设计奖惩激励机制对节点行为进行实时处理。

(3)通过仿真软件测试本文提出的区块链系统,实现节点的分级处理、区块的生产与验证流程,并与不同方案对比。实验结果表明此方案在抗操纵性、节点投票积极性、安全性等方面性能优于传统DPoS共识算法。并且相较目前主流改进方案拥有更高的去中心化水平和公平性。

1 基于多级委员会的区块链架构

本文提出了一种基于多层级委员会的新型区块链架构模型,旨在通过对区块链节点的属性判断、行为分析和动态划分,从抗操纵性、节点参与共识积极性、区块链去中心化程度及安全性等方面提升区块链系统的性能,具体如图1所示。将加入区块链的网络节点分为恶意、普通和高分节点,以委员会层级结构的方式进行节点判别与功能划分。各层级分别为:网络公共节点池、次级委员会、出块委员会和验证委员会,代表着节点在区块链系统中的不同状态和分工。由a到e共5个模块进行节点的挑选与判断,各模块详细介绍如下:

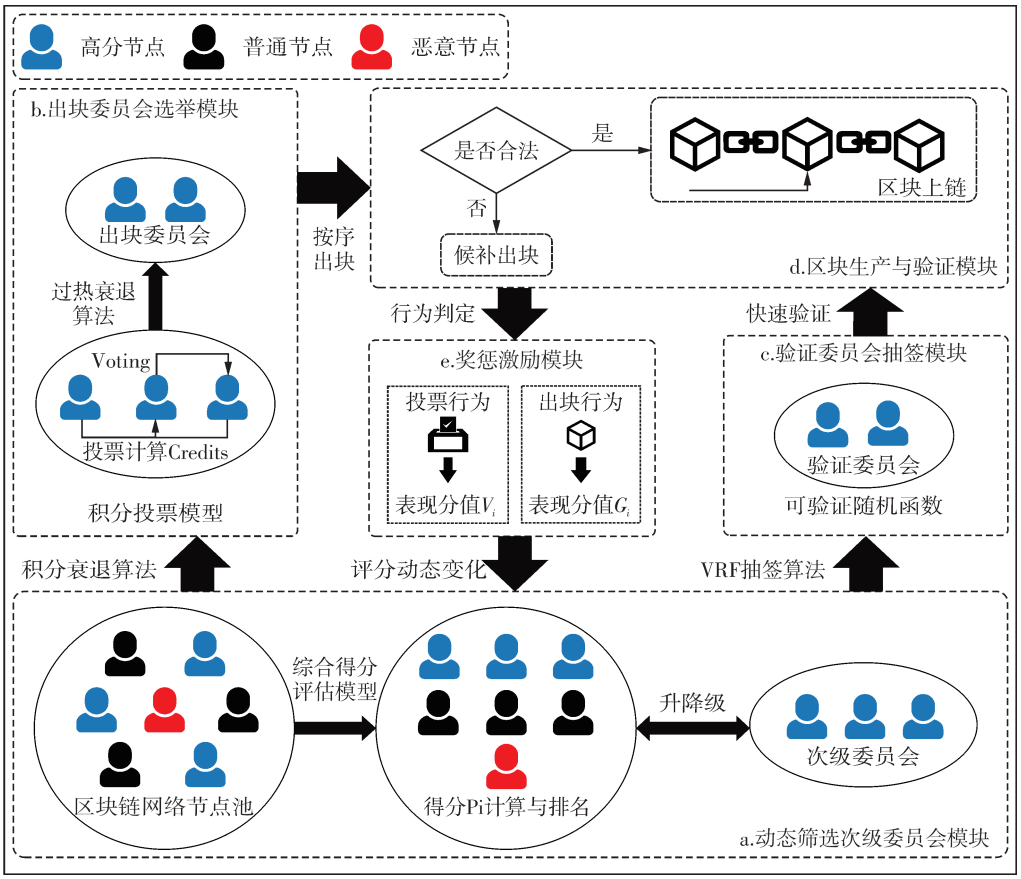


图 1　多级委员会系统模型图

1.1　动态筛选次级委员会模块 a

区块链系统在网络节点中挑选可靠的节点生产区块,但直接选择见证节点轮流出块极易导致巨型节点垄断现象[18],同时固定的出块节点也更容易被预知出块者并进行操控攻击,严重影响了系统安全性,因此本文在多级委员会架构中设计次级委员会选举算法对网络节点进行预选。

算法会在每一轮共识开始选举见证节点出块之前进行系统预选,通过预先设定的去中心化指标(Decentralization Metrics, DM)划定次级委员会节点数 n,筛选出拥有较高信誉值、代币储量和网络性能的节点进入委员会,并对节点的各项属性综合评估并计算得分,得分排名靠前的 n 个节点在这一轮中入选次级委员会。具体算法流程详见 2.1 节。

1.2　出块委员会选举模块 b

基于 DPoS 改进的共识机制普遍存在去中心化程度低的问题,本文设计了积分衰退算法以实现在挑选可靠节点的同时将权利下放给网络中的更多节点。

具体而言,通过模块 a 产生的次级委员会将在内部利用积分投票模型进行投票,平衡出块节点票数。模块 b 利用过热衰退算法计算每个节点的实际积分,与 EoS、Steem 等主流区块链项目相同,选举积分最高的 21 个节点进入出块委员会。这样的节点选取被证明规模足够小能够快速完成共识,同时防止严重的中心化。此流程为更多的节点提供出块机会,提高共识机制的公平性,具体算法流程详见 2.2 节。

1.3　验证委员会抽签模块 c

DPoS 仅选出固定见证节点生产并验证区块,导致参与共识的节点较少,存在安全隐患问题,本文利用可验证随机函数(Verifiable Random Function, VRF)抽签算法动态选举验证委员会。

模块 c 抽签选择节点进入验证委员会,对打包的区块进行合法性验证。动态选择验证节点保障共识过程的安全性,此外更小更明确的验证组成员也提供了更高的验证效率,具体算法流程详见 2.3 节。

1.4　区块生产与验证模块 d

模块 d 具体内容为出块委员会节点按照积分排序进行出块,并将区块信息打包广播给验证委员会节点进行区块合法性验证。若共识规定时间内没

有生成有效区块或验证未通过则在次级委员会剩余节点中挑选合适节点作为候选节点代替出块。具体算法流程详见2.3节。

1.5 奖惩激励模块e

针对DPoS算法中见证节点获取出块奖励,累积权益占比导致其余节点难以选拔为见证节点,以及节点消极投票或恶意投票操纵排名等问题,模块e设计了奖惩激励机制对节点行为进行处理以提高节点投票积极性并快速剔除恶意节点。具体算法流程详见2.4节。

2 MC-DPoS共识算法

本节将介绍MC-DPoS共识算法,基于第1节所提出架构中各个模块进行更详细的算法设计。MC-DPoS算法在DPoS投票选举出块节点的基础上,将网络节点利用委员会进一步分层,拆解见证节点权利,重新设计选举与区块生产、验证的流程,同时引入适配委员会架构的奖惩激励机制,在抗操纵性、节点投票积极性、安全性等方面针对DPoS的不足进行优化。

2.1 次级委员会选举算法

次级委员会作为预选组织,需要通过收集并综合考虑节点自身的各项属性,如自身权重、网络性能、信誉表现评价等,来对节点进行综合评价。因此,本文定义了一种节点综合得分评估模型$P(P_w,P_c,P_r)$,具体如下:

节点自身权重得分P_w^i:节点自身权重与PoS共识机制中自身权重意义相同,节点自身权重得分计算方式如式(1)和式(2)所示。

$$W_i = \frac{T_i}{\sum_{i=1}^{N} T_i} \tag{1}$$

$$P_w^i = \frac{W_i}{W_{\mathrm{MAX}}} * 100 \tag{2}$$

其中,W_i表示节点i($i \in [1,N]$)拥有代币权益占全部网络节点代币总量的比重,W_{MAX}表示拥有最高自身权重得分的节点权重,T_i为节点拥有的代币数量,N为网络节点总数。由以上公式可以看出,拥有越多的网络代币权益的节点,自身权重越高。

性能得分P_c^i:节点性能主要表现为节点i网络通信能力,可以利用节点在线时长来体现节点的性能指标。量化节点网络性能如式(3)所示。

$$P_c^i = \frac{1}{\mathrm{e}^{t-t_i}} * 100 \tag{3}$$

其中,t为上一轮共识所用总时长,t_i为节点i在一轮共识中的在线时长,节点在线时长越长,则拥有更高的性能得分,反之则更低。

信誉表现评价得分P_r^i:信誉表现评分的计算方式如式(4)所示。

$$P_r^i = P_0 + V_i + G_i \tag{4}$$

其中,P_0为节点加入区块链网络初始信誉值得分,V_i和G_i分别为节点i投票行为和出块行为的表现分值变化,他们代表了节点的不同行为对节点信誉值的影响,该影响将在3.5节奖惩机制中详细说明。

综合P_w^i、P_c^i、P_r^i得分,最终得到节点综合得分评估模型$P(P_w,P_c,P_r)$如式(5)所示。

$$P_i = \alpha P_w^i + \beta P_c^i + \gamma P_r^i \tag{5}$$

其中,参数α、β、γ分别为P_w^i、P_c^i、P_r^i所占的权重,且$\alpha + \beta + \gamma = 1$。将多种因素纳入节点综合得分评估模型并分配不同的权重,可以更全面地挑选出拥有良好信誉并且有作为出块节点能力的节点进入次级委员会参与进一步共识。

根据节点综合得分评估模型,在每一轮共识开始时收集节点信息。根据不同区块链网络中对节点属性的不同需求设定α,β,γ权重值,更新所有网络节点得分P_i,并降序排序,选择以当前DM值确定数量为n的节点加入次级委员会。由于每一轮节点i的行为都将引起P_i的变化以及公有链中节点自由进出特性,区块链网络中的节点在每一轮都有可能面临次级委员会中的升降级,这将不断刺激节点提高自身性能以及进行积极的行为。

2.2 积分衰退算法

本节通过为次级委员会设计积分衰退投票算法来解决节点垄断与去中心化水平低的问题。其中,积分衰退算法由积分投票模型与过热衰退算法两部分组成。

2.2.1 积分投票模型

系统为次级委员会中的每一个节点i统计积分,当获得网络中节点的投票时,节点i获得与被投票数等量的积分值,记为Cre_i。在投票阶段结束后,统计积分值,由排名前21的节点入选出块委员会并在下一个阶段完成出块工作。

入选出块委员会的节点在完成一轮共识中的出块任务后,排名最后的节点清空积分值,其余节点扣除等量积分,实现对出块节点的控制。次级委员会中其他节点积分值不变,累积到下一轮共识投票中。可以有效防止高票节点的积分累积,同时对持续保持次级委员会席位的低票优秀节点累加积

分,让更多节点拥有生产区块的机会。

通过引入积分投票机制,拥有较少投票数的节点也能通过不断累积积分入选。此方案可以在多级委员会环境中让更多优秀节点拥有出块机会,极大提高了去中心化水平,但持续高票节点仍可能长期垄断出块节点。

2.2.2　过热衰退算法

为了进一步解决积分投票模型中存在的垄断现象,本文受文献[18]启发,设计过热衰退算法按照连续出块轮次持续对节点积分进行衰退,避免个别节点的积分累积过高影响系统去中心化水平以及恶意投票操纵节点排名行为,详细方案如下:

(1) 以多级委员会架构共识机制为基础的区块链系统在次级委员会投票阶段利用积分投票模型进行投票,投票阶段后节点 i 获得积分为 Cre_i。

(2) 对上一轮前 21 名被选入出块委员会的节点进行积分衰退,定义过热衰退后节点 i 的积分为 Cre_i',利用式(6)进行计算得到 Cre_i'。

$$Cre_i' = Cre_i * f(r) \tag{6}$$

其中,$f(r)$ 为衰退函数,如式(7)所示。

$$f(r) = \exp\left(-\frac{r^2}{k}\right) \tag{7}$$

其中,r 为节点 i 连续出块轮次计数,节点 i 每进入一次出块委员会 r 增加 1。k 为冷却系数,即为节点 i 的出块“热度”降温速率。$f(r)$ 值域为(0,1]。

2.3　VRF 抽签算法与出块验证

为了保障数据共享的安全性,由动态验证委员会成员对生成的新区块进行验证。验证节点承担起整个区块链系统的安全保障,为避免恶意节点成为验证节点,动态验证委员会由次级委员会成员选举,起到对节点预选作用。系统规定出块委员会与验证委员节点成员不允许重合,保证权利分离。本文采用 VRF 可验证随机函数抽签算法,在每一轮出块委员会选举完成后抽签选择验证委员会节点。

出块委员会和验证委员会节点选取后完成,将进行区块的生产与验证,详细节点参与共识流程如图 2 所示。

2.4　奖惩激励机制

为了快速判断并剔除恶意节点,本文针对节点的投票行为和出块行为设计了奖惩激励机制。其中对节点的奖惩主要分为信誉表现评价分以及积分值两部分,同时为了提高节点作恶成本,要求次级委员会节点成员缴纳押金。

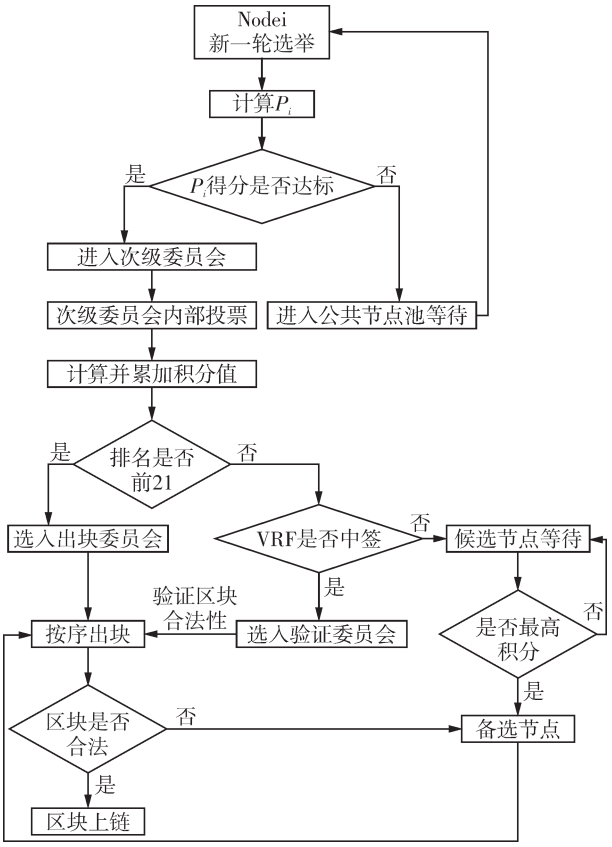


图 2　节点参与共识流程图

2.4.1　投票行为

节点投票行为有 3 种,积极投票给良好节点记为 v_i^a;消极投票记为 v_i^p;恶意投票,投票给异常出块节点记为 v_i^m。

一轮共识完成后,统计节点投票行为,对于积极投票和消极投票节点利用式(8)和式(9)计算投票行为分值 V_i。

$$v_i = v_i^a - v_i^p \tag{8}$$

$$V_i = R_V * \frac{1 - e^{-\varepsilon v_i}}{1 + e^{-\varepsilon v_i}} \tag{9}$$

其中,v_i 为节点 i 积极投票与消极投票的差值。式(9)利用 Sigmoid 函数变化得来,R_V 为投票行为占信誉表现行为得分中的变化分值,ε 为奖惩力度参数,节点投票行为为节点信誉表现评价带来正负 R_V 的分值变化。

对于恶意投票行为,系统容忍投票给恶意行为次数为 3 次,每次恶意投票行为直接扣除 $R_V/3$,节点 V_i 为 $-R_V$ 分则将节点 i 剔除系统。

2.4.2　出块行为

节点出块行为分为两种,正常出块记为 g_i^a,异常出块记为 g_i^m。

对于正常出块行为,在一轮共识完成后返还押

金,给予相应代币奖励记为E_i,计算方式如式(10)所示,并且获得正向信誉表现评价变化。出块行为信誉表现评价G_i计算方式如式(11)所示。

$$E_i = \frac{D_i}{\sum_{j=1}^{N} D_j} * F \tag{10}$$

$$G_i = R_G * \frac{1 - e^{-\mu g_i}}{1 + e^{-\mu g_i}} \tag{11}$$

其中,式(10)中F为每轮系统进行出块奖励的总代币金额,D_i为节点i缴纳的押金金额,节点根据缴纳押金占总押金比重获取相应的报酬。式(11)中g_i为节点i正常出块次数,R_G为出块行为占信誉表现行为得分中的变化分值,μ为奖惩力度参数。

对于异常出块行为,扣除其所有押金并获得负向信誉表现评价变化。系统进行严格的恶意节点剔除,仅容忍一次异常出块行为,将节点出块行为得分置为$-R_G$,若节点拥有两次异常出块记录则判定为恶意节点剔除系统。

3 实验分析

3.1 实验环境

为验证基于多级委员会架构的共识机制(MC-DPoS)在区块链系统中的各项性能指标,本文设计了相关仿真实验。实验环境为Windows11操作系统,Core i7-13650hx处理器,32 GB内存,开发环境为Goland,编程语言为Golang1.21。

3.2 参数设置

设计仿真区块链系统共200个网络节点,参照EoS区块链项目选定21个节点为出块委员会节点[20],考虑到公有链节点进出,每轮共识结束随机2个节点进入与离开系统,其他实验参数设计如表1所示。

表1 实验设置参数表

标识符	含义	数值
N	网络节点总数	200
α	自身权重得分权重	0.3
β	性能得分权重	0.3
γ	信誉表现得分权重	0.4
P_o	初始信誉值得分	50
R_V	投票行为变化分值	15
G_V	出块行为变化分值	35
ε	投票行为奖惩力度	0.2
μ	出块行为奖惩力度	0.5

注:定义去中心化程度指标DM为次级委员会节点数量占总节点数量比值,如式(12)所示。

$$DM = \frac{n}{N} \tag{12}$$

在实际区块链系统中,次级委员会成员越多,去中心化水平越高。但导致次级委员会节点各项指标较低,恶意节点进入委员会概率较高,系统安全性降低,过多委员会节点则使得共识退化为普通DPoS。为了提高公平性,让可靠的节点都拥有出块的机会,需要控制节点个数,在保证DM尽可能高的前提下,筛选掉分数较低的节点,同时可以激励未选入委员会的节点提升自己的属性以加入委员会。实验考虑不同次级委员会数量对应不同DM值情况下,次级委员会内部节点平均分值变化情况,实验结果如图3所示。

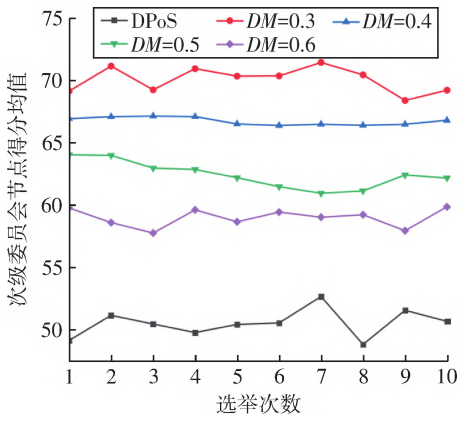


图3 不同DM下次级委员会节点平均综合得分

对比10轮共识选拔中DPoS和在MC-DPoS中不同DM值对应的平均得分可以观察到,次级委员预选机制可以选拔出节点评估得分更高的节点参与后续的共识,保障系统安全性。更低的DM值将带来更高的节点评分回报及系统安全性。因此,在后续实验选取DM=0.4,80个次级委员会节点进行,在保障DM不过低的基础上尽可能维持平均得分的稳定。

3.3 实验结果与分析

3.3.1 去中心化水平分析

实验将新共识方案与DPoS、HADPoS(Heat Attenuation Delegated Proof of Stake)、DPoSB(Delegated Proof of Stake with Nodes Behavior and Borda Count)、CW-DPoS(Credit-Weighted Delegated Proof of Stake)[21]进行对比。在同等区块链环境下进行50轮次共识,实验结果如图4所示。

由图4可知,DPoS共识在累积一定轮次投票之后出块节点基本固定,在本文的实验环境下,参与出块节点仅占30%。HADPoS、DPoSB和CW-DPoS

算法均在一定程度上改善了这种情况，分别使参与出块节点占比提高了20%、25%和19%，但依然有许多可靠节点没有被选为出块节点的机会。而MC-DPoS算法在排除了筛选不通过的劣质节点和系统判断恶意的节点后，仍有约70%的网络节点拥有出块的可能。实验表明，MC-DPoS算法较好地提高了区块链系统的去中心化水平与公平性，相较于HADPoS、DPoSB和CW-DPoS算法，分别提升了约40%、27%和42%的节点参与出块率。

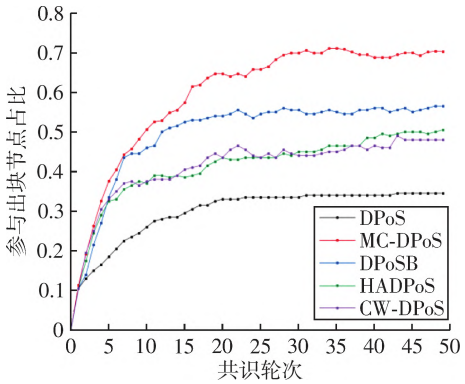


图4　不同共识参与出块节点数量对比

3.3.2　抗操纵能力分析

为了验证本方法的抗操纵能力，实验对第一轮投票选举中排名为40的节点进行操纵。分别采用DPoS，仅使用过热衰退机制，仅使用积分制度以及新共识方法进行测试，测试方式为在每一轮投票共识中分别为该节点增加4 000，6 000，8 000，10 000票模拟节点贿赂投票行为或操纵节点行为，观察在不同方案下节点在委员会（竞选节点）中排名的变化，进入前21名则意味着该节点本轮被选为出块节点，图5为增加8 000票数时的节点排名变化图。统计10次实验中初始排名40的节点平均出块次数如表2所示。

由图5及表2可知，在恶意操纵投票下，DPoS中节点排名迅速上升垄断见证节点。仅过热衰退机制下节点排名快速上升，票数衰退后排名下降，但停止出块后依然会攀升回较高的排名。仅积分制下节点排名上升较缓，但累积积分值至前端后仍会存在垄断现象。在MC-DPoS算法中，节点并不会在短时间内拥有出块机会，而过热衰退机制也有效遏制了节点的长期出块，在恶意操纵情况下获得了最少的出块次数。

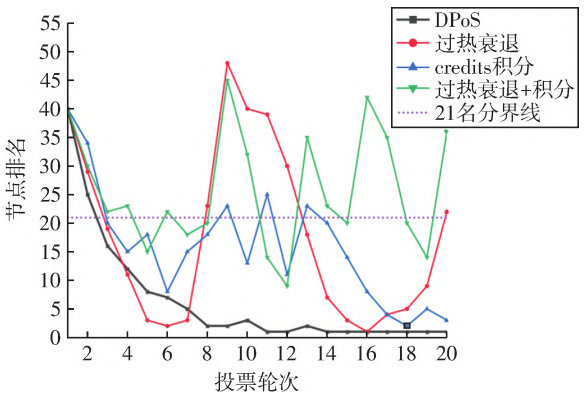


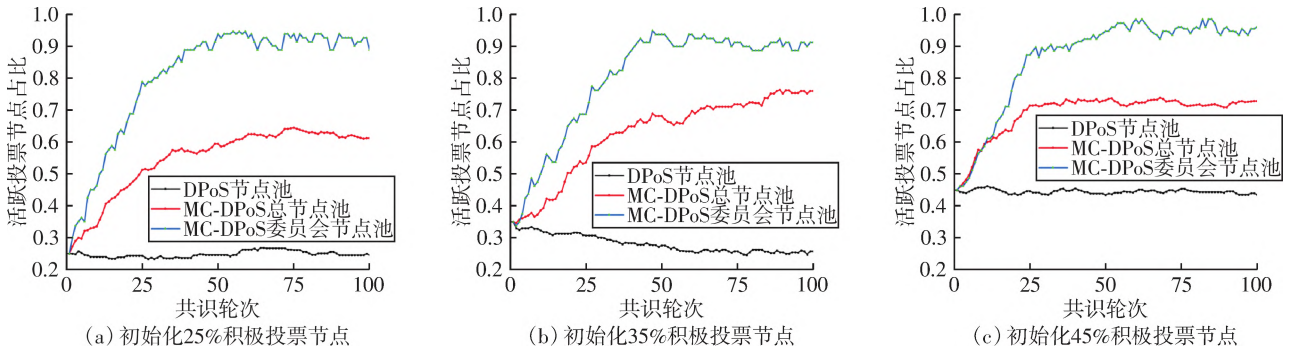
图5　额外票数8 000时不同算法排名40节点排名变化图

表2　不同额外票数下各算法排名40节点出块次数

额外票数	DPoS	仅过热衰退	仅积分制	MC-DPoS
4 000	14	8	8	4
6 000	17	10	11	5
8 000	18	12	15	8
10 000	19	13	17	10

3.3.3　节点投票积极性分析

实验对比在DPoS以及MC-DPoS算法下的活跃投票节点占比，定义活跃投票节点为：投票次数与进入次级委员会次数比值大于60%[13]。分别初始化25%、35%和45%的积极投票节点，实验进行100轮共识，统计DPoS共识节点池，MC-DPoS共识中总节点池和次级委员会节点池中活跃投票节点的占比，实验结果如图6所示。



（a）初始化25%积极投票节点　（b）初始化35%积极投票节点　（c）初始化45%积极投票节点

图6　活跃投票节点占比

由图6可知,DPoS积极投票节点占比基本不变。而在MC-DPoS算法中节点拥有更高的节点投票积极性,在次级委员会节点中投票积极性会更高,超过90%的节点会在每一轮投票选举中进行投票。奖惩激励机制以及更大的出块机会会激励节点积极投票。实验表明,MC-DPoS算法中,普通节点和委员会节点均有更高的投票积极性。

3.3.4 恶意节点剔除速率分析

实验统计DPoS算法中恶意节点占比,MC-DPoS中恶意节点在总节点池及次级委员会节点池中的占比。系统初始化30%的恶意节点,动态加入的节点拥有同样概率成为恶意节点,在进行投票和出块行为时会进行异常操作,实验进行30轮共识,结果如图7所示。

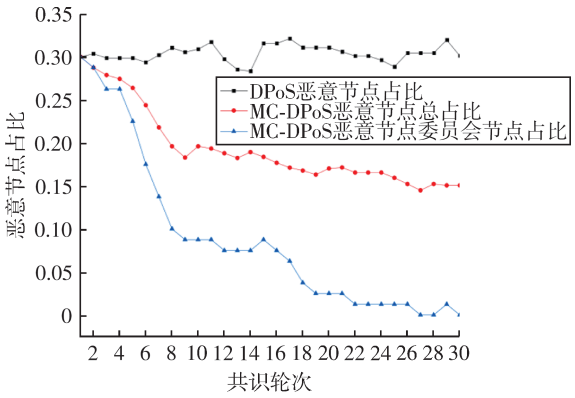


图7 恶意节点占比

30轮共识后,DPoS异常节点占比基本没有变化,而MC-DPoS中恶意节点被快速剔除,约有50%恶意节点被剔除总节点池,在次级委员会中,恶意节点会得到更严格的降级处理,最终全部清除。实验表明,MC-DPoS共识机制降低了节点作恶的可能,拥有更高的安全性。

4 结束语

本文提出一种区块链中基于多级委员会的去中心化节点管理方法,并基于此设计MC-DPoS共识算法,通过仿真实验验证其可行性,该方法可为物联网、金融交易等领域中的中心化、公平性问题提供可靠的解决方案。通过提出综合得分评估模型,动态选举出更可靠的次级委员会节点,降低节点作恶的可能。通过设计积分投票模型以及改进过热衰退算法选举出块委员会节点,防止垄断现象的发生,有效提高了网络节点出块的公平性,保证了区块链去中心化水平,并在一定程度上提升了系统的抗操纵能力。利用VRF抽签算法实现可信区块的快速验证,提高了安全性。通过设计奖惩机制,实现对恶意节点的快速剔除,进一步提高节点投票积极性。

参考文献:

[1] ZHENG Z B, XIE S A, DAI H N, et al. Blockchain challenges and opportunities: a survey[J]. International Journal of Web and Grid Services, 2018, 14(4): 352.

[2] 刘晨磊, 孙语蔚, 王梓炫, 等. 基于区块链的软件定义网络数据安全共享研究进展[J]. 南京邮电大学学报(自然科学版), 2024, 44(5): 72-86.
LIU Chenlei, SUN Yuwei, WANG Zixuan, et al. Review on secure data sharing in blockchain-based software defined networks[J]. Journal of Nanjing University of Posts and Telecommunications (Natural Science Edition), 2024, 44(5): 72-86. (in Chinese)

[3] 孙国梓, 万明发, 王钰, 等. 区块链交易隐私保护技术研究进展[J]. 南京邮电大学学报(自然科学版), 2024, 44(4): 30-43.
SUN Guozi, WAN Mingfa, WANG Yu, et al. A survey on privacy protection technology for blockchain transactions[J]. Journal of Nanjing University of Posts and Telecommunications (Natural Science Edition), 2024, 44(4): 30-43. (in Chinese)

[4] DECKER C, SEIDEL J, WATTENHOFER R. Bitcoin meets strong consistency[C]//Proceedings of the 17th International Conference on Distributed Computing and Networking. 2016: 1-10.

[5] MENG T H, ZHAO Y B, WOLTER K, et al. On consortium blockchain consistency: a queueing network model approach[J]. IEEE Transactions on Parallel and Distributed Systems, 2021, 32(6): 1369-1382.

[6] LI W Y, FENG C L, ZHANG L, et al. A scalable multi-layer PBFT consensus for blockchain[J]. IEEE Transactions on Parallel and Distributed Systems, 2021, 32(5): 1146-1160.

[7] LEI K, DU M Y, HUANG J Y, et al. Groupchain: towards a scalable public blockchain in fog computing of IoT services computing[J]. IEEE Transactions on Services Computing, 2020, 13(2): 252-262.

[8] ANTONOPOULOS A M. Mastering Bitcoin: Unlocking Digital Crypto-Currencies[M]. Sebastopol: O'ReillyMedia, 2014: 173-214.

[9] SAAD M, QIN Z, REN K, et al. E-PoS: making proof-of-stake decentralized and fair[J]. IEEE Transactions on Parallel and Distributed Systems, 2021, 32(8): 1961-1973.

[10] LARIMER D. Delegated proof-of-stake white paper[EB/OL]. [2024-04-20]. https://bitshares.org/delegated-proof-of-stake-consensus.

[11] WEI Y X, LIANG L, ZHOU B, et al. A modified blockchain DPoS consensus algorithm based on anomaly detection and reward-punishment[C]//13th International Conference on Communication Software and Networks (ICCSN). 2021: 283-288.

[12] EL RHARBI N, ATTERIUAS H, YOUNES A, et al. A comparative study of the recent blockchain consensus algorithms[C]//Proceedings of the International Conference on E-Learning and Smart Engineering Systems (ELSES). 2023: 316-327.

[13] LI W C, DENG X H, LIU J, et al. Delegated proof of stake consensus mechanism based on community discovery and credit incentive[J]. Entropy, 2023, 25(9): 1320.

[14] 侯凯祥, 邱铁, 徐天一, 等. 带有预验证机制的区块链动态共识算法[J]. 软件学报, 2024, 35(5): 2485-2502.
HOU Kaixiang, QIU Tie, XU Tianyi, et al. Dynamic blockchain consensus with pre-validation[J]. Journal of Software, 2024, 35(5): 2485-2502. (in Chinese)

[15] XU G X, LIU Y, KHAN P W. Improvement of the DPoS consensus mechanism in blockchain based on vague sets[J]. IEEE Transactions on Industrial Informatics, 2020, 16(6): 4252-4259.

[16] 付晓东, 漆鑫鑫, 刘骊, 等. 基于权力指数的DPoS共谋攻击检测与预防[J]. 通信学报, 2022, 43(12): 123-133.
FU Xiaodong, QI Xinxin, LIU Li, et al. Detecting and preventing collusion attack in DPoS based on power index[J]. Journal on Communications, 2022, 43(12): 123-133. (in Chinese)

[17] TAN C, XIONG L. DPoSB: delegated proof of stake with node's behavior and Borda count[C]//IEEE 5th Information Technology and Mechatronics Engineering Conference (ITOEC). 2020: 1429-1434.

[18] YOU C, QIN Y J, CHEN Q, et al. HADPoS: improvement of DPoS consensus mechanism based on heat attenuation[J]. IT Professional, 2023, 25(1): 40-51.

[19] WANG B C, LI Z T, LI H B. Hybrid consensus algorithm based on modified proof-of-probability and DPoS[J]. Future Internet, 2020, 12(8): 122.

[20] LI C, XU R H, DUAN L. Liquid democracy in DPoS blockchains[C]//Proceedings of the 5th ACM International Symposium on Blockchain and Secure Critical Infrastructure. 2023: 25-33.

[21] WANG B, LI H L, PAN L. Optimized DPoS consensus strategy: credit-weighted comprehensive election[J]. Ain Shams Engineering Journal, 2023, 14(2): 101874.

(责任编辑:李小溪)