基于综合积分机制的权益证明共识算法改进研究

鲁明[1,3]，陈慈发[1,3*]，董方敏[1,2,3]

（1. 三峡大学湖北省建筑质量检测装备工程技术研究中心，湖北 宜昌 443002；
2. 三峡大学水电工程智能视觉监测湖北省重点实验室，湖北 宜昌 443002；
3. 三峡大学计算机与信息学院，湖北 宜昌 443002）

摘　要：共识机制是区块链的核心。权益证明（PoS）作为一种共识机制，与工作量证明（PoW）相比显著降低了资源的消耗。但 PoS 中积极的低权益诚实节点难以获得记账权，除此之外，还存在节点区块验证不积极、币龄累计攻击和出块奖励分配不合理的安全问题。为此，提出了一种基于 PoS 的改进方案。首先，通过引入积分机制来提升积极的低权益诚实节点的总权益，提高节点获得记账权的概率；其次，采用非线性函数进行币龄计算，防止恶意节点累计币龄发动攻击；最后，根据节点综合积分占比分配出块奖励，在规定时间内积极参与验证或投票的节点会得到奖励，减少“富者越富”现象，缩短节点之间的贫富差距。实验结果表明，相比其他 PoS，所提的改进共识机制有效控制币龄的无限增长，积极的低权益诚实节点获得奖励和记账权的次数提升了约 3.6 倍和 2.6 倍，降低了系统的中心化趋势，增大了积极的低权益诚实节点的竞争记账权的机会和减小了币龄攻击的可能性，进一步验证了所提方案的可行性和优越性，促进了区块链网络的健康发展。

关键词：共识机制；区块链；权益证明；积分值机制；非线性函数；出块奖励分配

源代码链接：https://gitee.com/lmingboy/go-code/tree/master/

中图分类号：TP391　　**文献标志码：**A　　**DOI：**10.19678/j.issn.1000-3428.0068678

Research on Improved Consensus Algorithm for Proof of Stake Based on Comprehensive Integral Mechanism

LU Ming[1,3], CHEN Cifa[1,3*], DONG Fangmin[1,2,3]

(1. Hubei Province Engineering Technology Research Center for Construction Quality Testing Equipment, China Three Gorges University, Yichang 443002, Hubei, China;
2. Hubei Key Laboratory of Intelligent Visual Monitoring for Hydropower Engineering, China Three Gorges University, Yichang 443002, Hubei, China;
3. College of Computer and Information Technology, China Three Gorges University, Yichang 443002, Hubei, China)

【Abstract】 The consensus mechanism is at the core of blockchain. Proof of Stake (PoS), as a consensus mechanism, significantly reduces resource consumption compared with Proof of Work (PoW). However, PoS still faces security issues, such as difficulty in obtaining accounting rights for active low-equity honest nodes, lack of active node block verification, coinage accumulation attacks, and unreasonable allocation of block rewards. Consequently, this study proposes an improved scheme based on PoS. First, an integral mechanism is introduced to enhance the total equity of active low-equity honest nodes and increase the probability of nodes obtaining accounting rights. Second, nonlinear functions are used for the coinage calculation to prevent malicious nodes from accumulating coinage and launching attacks. Finally, using a proportion of comprehensive points of nodes to distribute block rewards, nodes that actively participate in verification or voting within a specified time receive rewards, thereby mitigating the phenomenon of "the rich getting richer" and the wealth gap between nodes. The experimental results show that compared to other PoS-improved consensus mechanisms, the proposed mechanism offers more effective control of infinite growth in coinage. The frequency at which the active low-equity honest nodes received rewards and accounting rights increased by 3.6 and 2.6 times, respectively. This reduces the centralization trend of the system, enhances the opportunities for active low equity honest nodes to compete for accounting rights, and reduces the possibility of coinage attacks. Further validation of the feasibility and superiority of the scheme has promoted the healthy development of blockchain networks.

【Key words】 consensus mechanism; blockchain; Proof of Stake (PoS); integral mechanism; nonlinear function; distribution of block rewards

收稿日期：2023-10-24　　**修回日期：**2024-01-17

通信作者 E-mail：*719207373@qq.com

0 引言

自 2009 年比特币[1]设计并实现以来，区块链已成为智能电网[2]、物联网[3]、医疗[4]、智能合约[5]等多个领域的技术平台。随着去中心化应用的不断发展，区块链的核心组件共识机制正成为性能的瓶颈。比特币引入了第 1 个共识协议工作证明(PoW)[6]，通过该协议，矿工不断计算新的哈希，直到它满足有效块预定义的条件。如今，PoW 几乎需要在 10 min 内进行 270 次哈希操作才能在比特币上生成 1 个数据块，这对于保证区块链[2]的安全至关重要，但同时也会造成巨大的能源浪费。为了解决这个问题，研究人员提出了提供类似于计算能力的安全保证的替代高效协议，如股权证明(PoS)[7]、活动证明[8]和空间证明[9-10]。

在所有针对 PoW 的替代协议中，PoS 能够避免计算开销，并以诚实的权益作为安全保证[11]。与 PoW 计算能力成正比的随机领导者选择过程相比，PoS 根据当前区块链状态，通过领导者选择算法选择与每个人所拥有权益成比例的利益相关者。为了保证安全性，需要在选择过程中引入熵。此外，采用最长链规则或拜占庭容错规则来确定 PoS 中唯一有效链。与 PoW 相比，PoS 生成块无须计算，因此在实践中设计和实现 PoS 仍然具有挑战性。

随着共识机制算法的不断改进和优化，共识达成性能也在不断提高。然而，相比其他共识机制，权益证明存在一些问题。首先，PoS 仅依赖节点权益大小来选择领导节点，导致诚实且权益较低的节点很难获得记账权，从而降低了它们的积极性；其次，PoS 面临币龄累计攻击[12]的问题，攻击者可以通过不断积累币龄来提高成为领导节点的概率，从而影响共识时间和效率；最后，在 PoS 中，权益较高的节点通常会获得更多的出块奖励，这可能导致权益集中化[13]，最终导致“富者越富，穷者越穷”的局面，严重削弱了区块链的去中心化程度并降低了公平性。

PoS 算法中积极的低权益诚实节点难以获得记账权，存在币龄累计攻击和节点奖励分配不合理等问题。为此，本文提出了一种改进的算法模型。首先，引入了积分机制，通过在有效时间内进行验证或投票区块操作，积极的低权益诚实节点可以获得积分来增加其总权益；其次，利用非线性回归函数计算币龄，并控制币龄的增长和上限，以应对币龄累计攻击。此外，对于积极参与共识的节点，赋予相应的收益奖励，从而激励诚实小节点的积极性。

1 相关研究

CHENG 等[14]在积分机制上使用积分将每个节点分级，作为每个节点的基本属性，提高较小节点的收益。LEONARDOS 等[15]通过相对于验证者投票行为和聚合区块奖励的算法权重作为积分值来优化集体决策。针对币龄累计攻击，LI 等[16]使用币的数量来选择矿工，同时采用线性函数来限制币龄的最大值。JIANG 等[17]将节点分成权益代表和矿工节点，根据节点参与创建区块的情况为节点分配可信度，应对币龄累计攻击。面对权益机制分配不公情况，SAHIN 等[18]为产生区块的节点分配一部分奖励，其余奖励则分配给所有节点。FANTI 等[19]利用几何奖励函数给部分区块分配奖励。BALA 等[20]为了减轻区块链参与者之间的不信任，在 PoS 的基础上提出了一种博弈论方法，该方法使用奖惩方案确保每个节点都能维护一定的信任阈值水平。MATSUNAGA 等[21]提出基于验证者投票的奖励机制。在此机制中，处罚而收取的权益会被重新分配到正确投票的验证者上，进一步提高了验证者为正确共识做出贡献的动机。DOU 等[22]提出了一种基于委员会的 PoS 协议，使用一个三阶段广播中介小工具和两个兼容性的确认规则，参与者可以定期调用三阶段广播，并根据不同的确认规则提交区块，解决了 PoS 协议中区块提交缓慢的问题。ANDREINA 等[23]提出一种新的权益证明协议，将投票权与权益以及 TEE 设备的所有权绑定在一起，根据可信执行环境的属性来限制恶意验证者的攻击，并采用前向安全等技术对后向破坏攻击进行保护。经过验证该协议是安全的，不会受到研磨攻击和远程攻击。

AKBAR 等[24]将 PoS 和 PoW 相结合。首先，使用 PoW 挖掘方法防止块生成时间超时；其次，生成的块通过 PoS 共识进行验证。该研究方法与以前的方法相比具有独特性和新颖型，除了能够处理 51%攻击以外，还能确保标准化分配采矿奖励。SAAD 等[25]提出了 e-PoS 模型，该模型将挖掘区块的机会分配给更多的利益相关者来缓解网络资源的集中化，并且通过惩罚恶意实体来实现公平采矿的目的。e-PoS 确保了 PoS 共识机制的公平性和去中心化。WANG 等[26]提出一个新的指标来量化激励相容性的水平，在几何奖励函数中添加随机盐作为 PoS 中一个新的奖励函数。通过比较，新奖励函数的公平性是最优的。GAO 等[27]针对 PoS 在应用过程中吞吐量不会随着网络扩展而增大的问题，在

PoS 的基础上添加了分片协议，分别将未经确认的交易和网络进行分片。网络分片并行处理交易分片以产生中间块，中间块被组合成链上区块。实验结果表明，该机制的吞吐量随着网络规模的增加而增大。

2 PoS 共识机制改进设计

传统的 PoS 共识机制中积极的低权益诚实节点难以获得记账权[14-15]，存在币龄累计攻击[16-17]、权益集中化和奖励分配的不公平性[18-19]问题。这些问题严重影响了整个区块链系统的安全性，违背了其去中心化的初衷。

为解决这些问题，本文对 PoS 共识算法进行了研究，并采用了创新性的技术手段，包括积分机制、非线性币龄计算算法和奖励分配算法等，对 PoS 共识机制进行了改进，从而提高了 PoS 共识机制的安全性，有效解决了币龄累计攻击问题，提高了参与共识节点的积极性，缓解了 PoS 共识机制算法的中心化问题。

2.1 综合积分机制设计

在原始的 PoS 共识机制算法中，参与领导节点竞选的节点需要质押一定数量的权益(代币)。当节点质押的权益经过时间的累积，币龄达到一定的标准后，节点大概率被选为领导节点，从而负责生成区块。因此，领导节点的币龄为质押的权益数与所质押时间的乘积，如式(1)所示：

$$C_{\text{Coinage}_i^h}=C_{\text{Coin}_i}\times T \tag{1}$$

式中：$C_{\text{Coinage}_i^h}$ 为参与第 h 轮共识机制中的节点 i 竞选记账权的币龄；C_{Coin_i} 为参与竞选的节点 i 质押的权益；T 为权益质押的时间。这种竞选领导节点的方式意味着节点所拥有的权益越多，越容易获得记账权。节点长期多次拥有记账权会加剧中心化。由于权益的集中，因此大大增加了节点作恶的概率。同时，币龄的计算方式容易导致节点遭受币龄累计攻击。

2.1.1 积分机制设计

在 PoS 中存在高权益节点会更倾向于保障系统安全的假设，该假设并非绝对成立。权益的集中会产生寡头垄断和操纵风险，从而影响系统的去中心化和安全性，这与区块链的本质特性相违背，同时也不能排除低权益节点对安全的共享。因此，采用不同的因素来平衡权益、权益分配和系统安全之间的关系，以确保系统的公平性、安全性和去中心化。在区块链中，除了本身包含无效信息的区块不能成功上链以外，还包含有效信息的区块经过分叉后被淘汰以及其他未获得竞争权的区块。这些区块虽然包含合法交易，但是在本轮共识结束后，由于未能上链，并不能使交易变成现实，因此本文将这些区块统称为非法区块。

本文将积分作为评选领导节点组成变量之一，通过积分可以有效反映节点参与共识的积极程度和诚实度，因此针对不同的节点行为设置不同的积分值。在文献[2,28]中，引入积分参数，仅仅通过积分来选择记账节点，除了积分并没有引入其他参数，评选标准过于单一。本文将节点积分和币龄组合的最终值作为竞选标准，同时为了计算简便，因此需要将积分和币龄设置成同一个数量级，并满足积分随着节点正确参与共识次数增加而增加的条件，同时不能远超过币龄。因此，节点积分的增加取自上一轮共识中领导节点币龄的一部分。采用标准化方法设计积分计算公式。积分计算公式如式(2)所示：

$$S_{\text{Score}_i^h}=\begin{cases}a\times C_{\text{Coinage}_{\text{winner}}^{h-1}}+S_{\text{Score}_i^{h-1}},\ T_i\leqslant\nabla T\&b_{\text{block}_i^h}=t_{\text{true}}\\ S_{\text{Score}_i^{h-1}},\ T_i>\nabla T\&b_{\text{block}_i^h}=t_{\text{true}}\\ 1,\ b_{\text{block}_i^h}=f_{\text{flase}}\end{cases} \tag{2}$$

式中：$S_{\text{Score}_i^h}$ 为第 h 轮共识后节点 i 获得的积分值；$S_{\text{Score}_i^{h-1}}$ 代表第 $h-1$ 轮共识后节点 i 的积分值；a 为占比参数；$C_{\text{Coinage}_{\text{winner}}^{h-1}}$ 为第 $h-1$ 轮共识节点 winner 获得记账权时节点的币龄；T_i 和 ∇T 为节点 i 参与共识时间和有效限制时间；$b_{\text{block}_i^h}$ 为在第 h 轮共识中节点 i 参与验证和投票的区块；当 $b_{\text{block}_i^h}=t_{\text{true}}$ 时，意味区块通过验证成为合法区块最终上链；当 $b_{\text{block}_i^h}=f_{\text{false}}$ 时，表示该区块未能成功上链，意味该区块是非法区块，因此对产生和验证投票该区块的节点进行惩罚，将该节点的积分值设置为 1。

为了获得积分，节点必须在有效时间 ∇T 内参与共识验证区块和投票，并且所验证和投票的区块必须成功上链。如果节点投票和验证的区块为非法区块，则节点的积分设置为 1，这大大增加了作恶节点的竞争难度。积分计算包含上一轮共识中一部分领导节点的币龄、自身累计积分和节点在共识中的行为表现等因素。该计算方法可以解决积分值和币龄数量级不同的问题，同时提高节点的积极性和参与共识的动力，从而提高整个系统的安全性。

2.1.2 综合积分评分模型设计

本文采用改进的柯布-道格拉斯生产函数[29]模型对节点进行综合积分计算，使竞选评分更加公平。

柯布-道格拉斯生产函数最早被广泛应用于经济学研究中。该函数参数估计与其他代数方程相比，计算过程比较方便且计算分析结论更准确。因此，本文最终采用柯布-道格拉斯生产函数作为计算节点综合积分模型，如式(3)所示：

$$Y=AL^{\alpha}K^{\beta} \tag{3}$$

式中：A 是综合技术水平参数，且 $A>0$；L 和 K 分别代表投入的劳动力和资金 2 种参数；α 和 β 分别为劳动力产出的弹性系数参数和资本产出的弹性系数参数，α 和 β 均大于 0，且 $\alpha+\beta=1$。该生产函数反映了在现实经济活动中，投入不同要素与产出的关系。

综合积分基于现有模型，将节点的币龄和积分作为关键要素，并根据实际情况对参数进行调整。通过综合计算这些要素得到 1 个数值，该数值被作为评选领导节点的判断依据，从而使记账权的评选更加合理。综合积分值作为评选领导节点的判断依据，可以解决单一因素产生偏差的问题，使记账权的评选公正、合理。通过这些改进提高共识机制的安全性，从而更好地服务于区块链的应用场景。

2.1.3 综合积分值重置机制设计

为了防止权益中心化，本文还设计了综合积分值重置机制。该机制可以避免少数节点长期被选为领导节点，导致综合积分值不断累积。具体来说，如果节点被选为领导节点并获得奖励后，在下一轮共识开始前，分别将节点的综合积分值、币龄和积分值重置为 0、1 和 1，这样可以保证领导节点的更替和轮换，促进节点积极参与共识。通过重置机制可以有效地提高 PoS 共识机制去中心化程度，降低权益的集中程度。该机制可以有效地防止少数节点长期占据领导节点的位置，从而使得更多节点有机会参与记账权的竞选。此外，重置机制也可以激励节点积极参与共识，避免节点懒惰和不诚实行为的出现。

综上所述，综合积分值重置机制可以提高 PoS 共识机制的安全性和去中心化程度。该机制通过限制领导节点的综合积分值，保证领导节点的更替和轮换，使得节点积极参与共识，从而更好地服务于区块链的应用场景。

2.1.4 非线性币龄计算方法

币龄累计攻击的基本思想是攻击者通过不断积累币龄，提高成为领导节点的机会，进而影响共识时间和区块增长率。为了有效防止币龄累计攻击，本文需要考虑以下 2 个方面：1)需要控制币龄增长的速度，使其随着时间的推移缓慢增加；2)需要设定币龄增长的上限。在这种情况下，logistic 回归模型可以满足上述要求。因此，本文提出基于 logistic 回归模型币龄计算方法，如式(4)所示：

$$C_{\mathrm{Coinage}_i}=C_{\mathrm{Coin}_i}\times\frac{1}{1+\mathrm{e}^{-T_i/100+0.5}}\times L_{\mathrm{Limit}} \tag{4}$$

式中：C_{Coinage_i} 是节点 i 的币龄；C_{Coin_i} 是节点 i 参与共识所质押的权益；T_i 为节点 i 所持权益质押的时间，由于 logistic 回归函数在对数增长期间数值增长是相当快的，不利于判断节点的币龄增长情况，因此将 T_i 修正为 $T_i/100$；L_{Limit} 为币龄的上限，根据具体情况进行调整。节点在质押一定数量权益后，随着质押时间的增加，节点 i 的 C_{Coinage_i} 增长速度逐渐减慢，最终限制在固定的数值。

2.2 激励机制改进

在传统 PoS 共识机制中，领导节点产生的区块成功上链后，节点会获得奖励。然而，由于每轮共识仅限领导节点获得奖励，因此在传统 PoS 共识机制系统中节点之间的“贫富”差距增大，即“富者越富”现象，加剧了系统的中心化，同时降低了低权益诚实节点的积极性。而权益集中于少部分节点上，也增加了这些节点作恶的可能性，进一步降低了系统的安全性。因此，本文提出一种新的奖励机制，重新分配奖励。

在共识过程中，节点参与记账权需要考虑币龄和积分值。高币龄和积分值意味着节点质押了更多的权益，并积极诚实地参与了区块的验证和投票。前者保证了系统的高效性，后者则保证了系统的安全性。因此，记账奖励应该根据节点的币龄和积分值进行分配，质押代币越多，积极诚实地参与区块验证和投票的积分值越高，分配相应的奖励也就越多。本文改进的激励机制计算过程如式(5)所示：

$$E_i=\begin{cases}E\times\dfrac{Y_i}{\sum\limits_{j=0}^{n}Y_j}, & S_{\mathrm{Score}_i}>1\\ 0, & S_{\mathrm{Score}_i}\leqslant 1\end{cases} \tag{5}$$

式中：E_i 为节点 i 获得的奖励；E 代表每轮共识结束后系统的总奖励；Y_i 表示节点 i 的综合积分值，包含节点的币龄和积分值 2 种因素；S_{Score_i} 表示节点 i 的积分值。

在改进激励方案中，当 $S_{\mathrm{Score}_i}\leqslant 1$ 时，意味着节点没有积极参与共识，或者节点是作恶节点，因此节点不应该获得奖励。同时，当多个节点的币龄相同时，积极诚实地参与共识次数越多的节点应获得更多的奖励。该分配方案有效缩短了节点之间的贫富差距，同时节点积极诚实地参与了共识，保证了系统

的安全性。

2.3 改进共识机制核心步骤

假设系统中有 N 个节点参与共识，共识周期为 T。本文改进共识机制的具体流程如图 1 所示。

1)参与记账权竞选的 N 个节点根据币龄和积分值计算得出节点的综合积分值。

2)根据节点的综合积分值高低竞选领导节点，综合积分值越高者成为领导节点的概率越高，成功当选的领导节点将负责打包交易以生成新的区块。

3)其余节点参与区块的验证和对领导节点产生的区块进行投票。

4)经过验证和投票的合法区块成功上链后，同时，对及时参与验证和投票该区块的节点增加积分值，对未能及时参与共识的节点积分保持不变；其他节点积分值置 1。最后，根据参与竞选时的综合积分分配区块奖励。

5)本轮共识结束，重复上述过程。

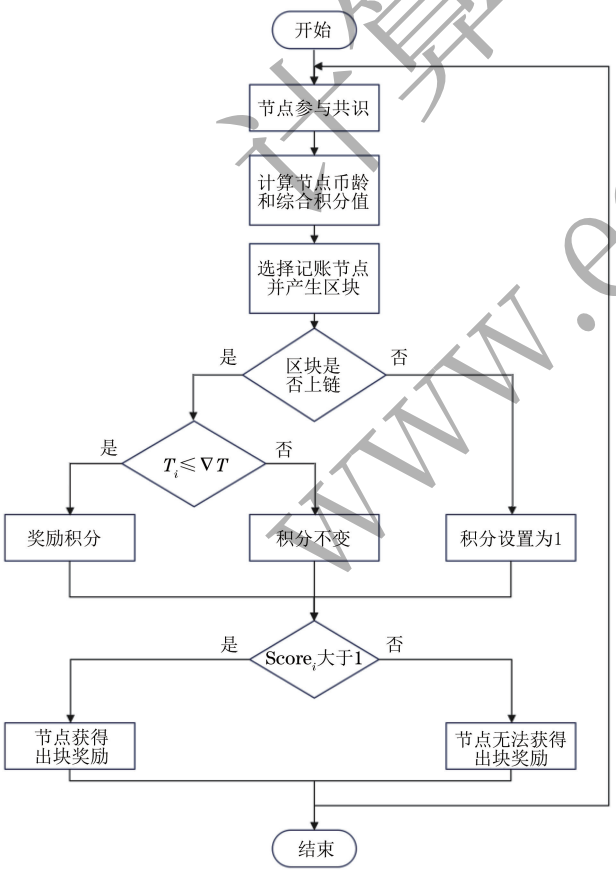

图 1 改进的共识机制流程

Fig. 1 Procedure of improved consensus mechanism

3 实验结果与分析

本文在实验配置为 Intel® Core™ i7-4790 CPU@ 3.60 GHz 处理器，8 GB 内存，64 位的 Ubuntu 20.04 系统下，编程语言为 Go 语言，模拟实现所提改进方案和其他方案。

为了解决传统 PoS 共识机制中的币龄累计攻击、收益算法分配不公以及积极的低权益诚实节点难以获得领导权的问题，本文提出了一种基于 PoS 共识机制的改进方案。为了验证该算法的效果，本文从 4 个方面进行分析：1)节点的币龄增长累计情况；2)奖励分配问题，重点分析获得的块奖励分红节点的数量；3)节点获得记账权的情况，重点分析的内容是在多轮次共识中不同节点获得记账权的次数；4)不同共识机制算法的计算开销对比。

3.1 币龄计算方式对比分析

为了验证新的币龄计算方式的合理性，在相同环境下，本文分别模拟了传统 PoS 共识机制的币龄计算方式和所提改进的币龄计算方式。在实验中，选择了 1 个诚实的积极性高的节点 a，分析在连续权益质押的时间内不同的共识机制币龄计算方式中币龄增长情况。实验结果如图 2 所示。

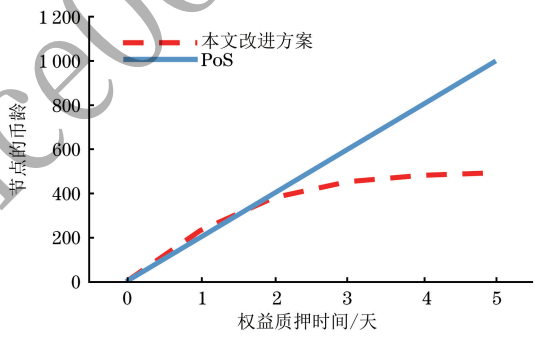

图 2 节点 a 在连续权益质押时间内的币龄变化

Fig. 2 The coins age change of node a during the continuous equity pledge period

从图 2 可以看出，在原始 PoS 共识机制中，节点 a 的币龄随着时间线性增加。而在改进后的共识机制中，节点 a 的币龄增长率随着权益质押时间的增加变低，最终币龄达到了稳定。这是因为传统的共识机制币龄计算方式采用线性函数，而改进后币龄的计算方式采用非线性回归函数，可以有效地抑制币龄的无限增加，对解决币龄累计攻击问题有显著的作用。

综上所述，改进后的币龄计算方式更加合理和有效，能够有效地防止币龄累计攻击，提高了共识机制的安全性和可靠性。

3.2 分红节点对比分析

在相同的实验配置下，本文分别模拟了多个节点在传统 PoS 共识机制、Incentive-PoS[30] 和本文改进方案中的奖励分配情况，实验结果如图 3 所示。从图 3 可以看出，传统 PoS、Incentive-PoS 和本文改进方案 3 种共识机制获得分红的节点数量情况：

$N_{本文改进方案}>N_{Incentive\text{-}PoS}>N_{PoS}$。这主要是因为本文改进的方案能够将及时参与共识验证和投票区块的低权益节点也纳入了分红范围，而传统 PoS 和 Incentive-PoS 并没有将积极的低权益诚实节点纳入分红范围，相对来说有失公平。

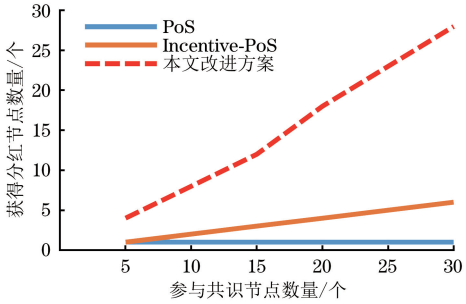

图 3 不同方案的奖励分配情况

Fig. 3 Reward allocation for different schemes

由于区块链网络中存在恶意节点或懒惰节点，因此一小部分节点未能获得奖励分红。然而，这恰好与改进方案的目的相吻合，减少了节点独享奖励的概率，避免出现“富者越富”的现象。同时，改进后的共识机制增加了节点参与共识的积极性和诚实性，节点只要积极诚实地参与验证区块和投票行为，就有机会获得奖励。

实验结果表明，改进后的 PoS 共识机制相较于传统 PoS 共识机制和其他方案，在奖励分配方面更加公平合理，增加了节点的积极性，并有效地解决权益中心化和出现不安全性的问题。

3.3 记账权竞争对比分析

本次实验在保证相同的配置下，分别采用 4 种不同类型的节点进行 50 轮共识机制实验。4 种不同类型的节点主要有积极的高权益诚实节点 node 1、懒惰的高权益作恶节点 node 2、积极的低权益诚实节点 node 3 和懒惰的低权益作恶节点 node 4，将以上节点分别在传统 PoS、Incentive-PoS 和本文改进方案的共识机制上运行，结果如图 4 所示。

从图 4 可以看出，传统 PoS 和 Incentive-PoS 共识机制中，记账权主要掌握在高权益节点（节点 node 1 和节点 node 2）中，而低权益节点获得极少的记账权次数。而本文改进的方案中，记账权主要掌握在积极的诚实节点（节点 node 1 和节点 node 3）中。传统的 PoS 和 Incentive-PoS 共识机制决定记账权的标准是币龄的大小，高权益节点拥有更高的权益和无上限的币龄累计，导致高权益节点在竞争记账权时具有较大的优势。相比之下，本文的改进方案采取了以下措施：1）每次高权益节点在获得记账权后，其综合积分值会被重置，

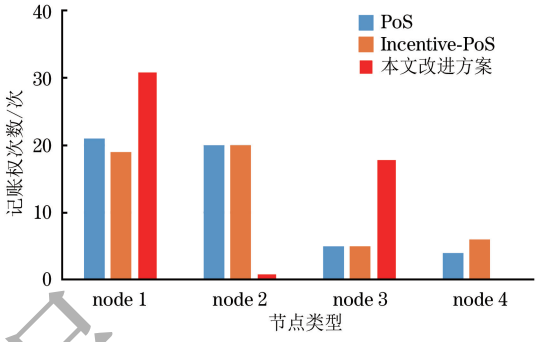

图 4 不同方案中节点获得的记账权次数

Fig. 4 The number of accounting rights obtained by nodes in different schemes

这意味着高权益节点需要从起点重新竞争记账权；2）通过改进币龄计算方式，限制了高权益节点的币龄增长；3）参与竞争的标准不仅仅取决于币龄，还取决于节点的积分值；4）对出块奖励进行分配，防止节点独享奖励。以上措施可以大大缩小了高权益节点和低权益节点之间的差距，相比传统的 PoS 共识机制，增加了积极的低权益诚实节点竞选记账权的机会。这意味着只要“勤奋和诚实就会有收获”，节点必须积极诚实地参与共识验证区块和投票，才能大概率地获得记账权。由此可见，本文的改进方案符合设计目的。

3.4 计算开销对比分析

在相同的实验配置下，本文分别模拟了传统 PoS 共识机制、Incentive-PoS 和本文改进方案在 50 轮共识中的执行时间和内存消耗，反映不同共识机制的计算开销。各共识机制的计算开销对比如表 1 所示。从表 1 可以看出，传统 PoS、Incentive-PoS、本文改进方案 3 种共识机制的计算开销：$O_{Incentive\text{-}PoS}>O_{本文改进方案}>O_{PoS}$。这主要是因为本文改进方案相比较传统方案增加了更多的计算公式，而在 Incentive-PoS 中添加的计算公式更加复杂，导致执行时间和内存消耗更多。

虽然本文改进方案的计算消耗相比原始方案 PoS 更多，但是本文改进方案的安全性和公平性具有更大的优势，尤其针对区块链的应用问题，安全性更加重要，同时针对计算机行业的快速发展，运算更加快捷。

表 1 各共识机制计算开销比较

Table 1 Comparison of computational costs among different consensus mechanisms

共识机制	执行时间/s	内存消耗/Byte
本文改进方案	50.025 9	19 632
Incentive-PoS	50.032 7	390 464
PoS	50.024 8	13 056

3.5 改进共识机制的性能分析

3.5.1 安全性分析

在改进的 PoS 共识机制中，节点积分作为竞选记账权的评价标准之一，如果节点恶意投票验证非法区块，其积分值将变为 1，该节点将很难获得记账权，从而排除了恶意节点，保证了节点之间的可靠性和安全性。同时，节点积分代表着节点在共识过程中的行为状态评价。由于偏离共识协议的节点共识行为具有任意性，因此本文设计的积分值方案具有对抗恶意共识行为的能力。

此外，本文的设计方案还保证了领导节点竞选的安全性，采用非线性回归函数的币龄计算方式，限制了节点的币龄累计，有效防止币龄累计攻击。同时，将币龄和积分值作为竞选标准，节点需要积极参与共识过程，为了获得更多的竞选机会，需要积极诚实地验证投票合法区块，从而保证了区块链中区块的安全性。

通过以上分析可以得出，本文的设计方案能够保证区块链系统的安全性。

3.5.2 一致性分析

改进的 PoS 共识协议在传统 PoS 共识机制的基础上实现了一致性，并通过积分值对节点参与共识的行为进行评估，保证了协议方案共识输出的一致性。在传统的 PoS 共识过程中，只要区块获得节点的 2/3 票数，就会被认为是合法区块，节点通过正常执行该协议来达成区块的共识一致性。改进后的 PoS 共识机制在传统机制的基础上进行了改进，维持了原有协议的一致性。同时，为了更公正地评估节点在共识过程中的表现，本文采用了积分机制。这一改进的共识机制通过积分来量化节点参与共识的行为。对于那些偏离共识协议的节点，它们将难以获得记账权，这是对其不当行为的惩罚。这样的设计确保了协议能够在大多数诚实节点的支持下顺利运行，并最终实现区块的一致性。

因此，本文所提的节点积分值能够保证共识达成一致性。

3.5.3 活性分析

本文改进的 PoS 共识机制的活性主要由共识过程中的视图切换和积分的迭代决定。在共识过程中，高综合积分的节点更容易被随机选择为领导节点，并且共识视图的编号是递增的。在节点接收到区块之后会进行区块验证。如果反对该区块的票数超过了总节点数量的 1/3，那么当前共识节点的一致性将无法达成。此时，系统将转向下一个视图的共识协议以继续尝试达成共识。在节点参与共识过程中，本文改进的共识机制通过限制币龄增加，使得大多数节点很容易达到币龄的最终值。因此高积分值成为节点竞选记账权的关键因素。在相同币龄的情况下，积分值越高的节点越容易获得记账权，而好的积分值代表了节点具有更高的可靠性。领导节点的可靠性降低了领导节点成为恶意节点的概率，从而增强了改进后 PoS 共识机制的活性。

4 结束语

传统 PoS 共识机制中积极的低权益诚实节点难以获得记账权，存在币龄累计攻击以及出块奖励分配不公平等问题。为此，本文提出了一种基于 PoS 的改进方案。首先，除了币龄以外，积分也成为选择领导节点的因素之一，有效地增加了积极的低权益诚实节点获得记账权的概率；其次，引入了非线性回归模型来计算币龄，有效地限制了币龄累计攻击；最后，出块奖励通过给节点二次分配，缩短节点之间的贫富差距，并激励节点积极参与共识。实验结果表明，本文改进后的 PoS 共识机制相较于传统的 PoS 机制更有效地防止了币龄累计攻击，维护了竞选的公平性，提高了节点的积极性，并更加合理地分配收益。通过对改进后 PoS 共识机制的安全性、一致性、活性和差异性的分析，本文方案相较于传统的共识机制在整体性能上有明显的提升，进一步维护了区块链系统的去中心化、可靠性和安全性，保证了区块链系统的健康发展。后续将不断提升共识机制的性能，在应对长程攻击、短程攻击以及提高区块吞吐量等方面，寻求共识机制更广泛的应用领域。

参考文献

[1] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[EB/OL]. [2023-09-21]. https://bitcoin.org/bitcoin.pdf.

[2] 涂园超，陈玉玲，李涛，等. 基于信誉投票的 PBFT 改进方案[J]. 应用科学学报，2021，39(1)：79-89.
TU Y C, CHEN Y L, LI T, et al. Improved PBFT scheme based on reputation voting[J]. Journal of Applied Sciences, 2021, 39(1): 79-89. (in Chinese)

[3] YAO H P, MAI T L, WANG J J, et al. Resource trading in blockchain-based industrial Internet of Things[J]. IEEE Transactions on Industrial Informatics, 2019, 15(6): 3602-3609.

[4] ZHANG A Q, LIN X D. Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain[J]. Journal of Medical Systems, 2018, 42(8): 140.

[5] LEI A, CRUICKSHANK H, CAO Y, et al. Blockchain-based dynamic key management for heterogeneous intelligent transportation systems[J]. IEEE Internet of Things Journal, 2017, 4(6): 1832-1843.

[6] DWORK C, NAOR M. Pricing via processing or combatting junk mail[C]// Proceedings of Annual International

Cryptology Conference. Berlin, Germany: Springer, 2007: 139-147.
[7] SOMPOLINSKY Y, ZOHAR A. Secure high-rate transaction processing in Bitcoin[C]//Proceedings of the 19th International Conference for Financial Cryptography and Data Security. Berlin, Germany: Springer, 2015: 507-527.
[8] BENTOV I, GABIZON A, MIZRAHI A. Cryptocurrencies without proof of work[C]// Proceedings of International Conference on Financial Cryptography and Data Security. Berlin, Germany: Springer, 2016: 142-157.
[9] BENTOV I, LEE C, MIZRAHI A, et al. Proof of activity: extending Bitcoin's proof of work via proof of stake[J]. Performance Evaluation Review, 2014, 42(3): 34-37.
[10] ATENIESE G, BONACINA I, FAONIO A, et al. Proofs of space: when space is of the essence[C]//Proceedings of the 9th International Conference of Security and Cryptography for Networks. Berlin, Germany: Springer, 2014: 538-557.
[11] DZIEMBOWSKI S, FAUST S, KOLMOGOROV V, et al. Proofs of space[C]// Proceedings of the 35th Annual Cryptology Conference. Berlin, Germany: Springer, 2015: 585-605.
[12] BENTOV I, LEE C, MIZRAHI A, et al. Proof of activity[J]. ACM Sigmetrics Performance Evaluation Review, 2014, 42(3): 34-37.
[13] NICOLAS H. It will cost you nothing to 'kill' a proof-of-stake crypto-currency[J]. SSRN Electronic Journal, 2014, 34(2): 1038-1044.
[14] CHENG Y, HU X H, ZHANG J G. An improved scheme of proof-of-stake consensus mechanism[C]//Proceedings of the 4th International Conference on Mechanical, Control and Computer Engineering (ICMCCE). Washington D. C., USA: IEEE Press, 2019: 8260-8263.
[15] LEONARDOS S, REIJSBERGEN D, PILIOURAS G. Weighted voting on the blockchain: Improving consensus in proof of stake protocols[J]. International Journal of Network Management, 2020, 30(5): e2093.
[16] LI A Y, WEI X H, HE Z. Robust proof of stake: a new consensus protocol for sustainable blockchain systems[J]. Sustainability, 2020, 12(7): 2824.
[17] JIANG Y H, ZHAO J Y, CHEN T W. Research on proof of stake consensus algorithm based on dynamic trust[C]// Proceedings of the 3rd International Conference on Signal Image Processing and Communication (ICSIPC 2023). Kunming, China: [s. n], 2023: 89-95.
[18] SAHIN H, AKKAYA K, GANAPATI S. Optimal incentive mechanisms for fair and equitable rewards in PoS blockchains[C]// Proceedings of the IEEE International Performance, Computing, and Communications Conference. Washington D. C., USA: IEEE Press, 2022: 367-373.
[19] FANTI G, KOGAN L, OH S, et al. Compounding of wealth in proof-of-stake cryptocurrencies[C]//Proceedings of International Conference on Financial Cryptography and Data Security. Berlin, Germany: Springer, 2019: 42-61.
[20] BALA K, KAUR P D. A novel game theory based reliable proof-of-stake consensus mechanism for blockchain[J]. Transactions on Emerging Telecommunications Technologies, 2022, 33(9): 4525-4529.
[21] MATSUNAGA T, ZHANG Y Y, SASABE M, et al. An incentivization mechanism with validator voting profile in proof-of-stake-based blockchain[J]. IEICE Transactions on Communications, 2022, 32(2): 228-239.
[22] DOU H Y, YIN L Y, LU Y, et al. A probabilistic proof-of-stake protocol with fast confirmation[J]. Journal of Information Security and Applications, 2022, 68: 103268.
[23] ANDREINA S, BOHLI J M, KARAME G O, et al. PoTS: a secure proof of tee-stake for permissionless blockchains[J]. IEEE Transactions on Services Computing, 2022, 15(4): 2173-2187.
[24] AKBAR N A, MUNEER A, ELHAKIM N, et al. Distributed hybrid double-spending attack prevention mechanism for proof-of-work and proof-of-stake blockchain consensuses[J]. Future Internet, 2021, 13(11): 285.
[25] 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.
[26] WANG Y L, YANG G Y, BRACCIALI A, et al. Incentive compatible and anti-compounding of wealth in proof-of-stake[J]. Information Sciences, 2020, 530: 85-94.
[27] GAO Y F, KAWAI S, NOBUHARA H. Scalable blockchain protocol based on proof of stake and sharding[J]. Journal of Advanced Computatioanl Intelligence and Intelligent Informatics, 2019, 23(5): 856-863.
[28] ZHAO M, HOU Y X, YU P, et al. Power companies labour scale demand prediction calculation model based on the COBB-Douglas function[C]//Proceedings of the International Conference on Cloud Computing, Big Data and Internet of Things (3CBIT). Washington D. C., USA: IEEE Press, 2022: 276-278.
[29] WANG J, GE L N. Consensus algorithm of proof-of-stake based on credit model[C]// Proceedings of the 4th International Conference on Blockchain Technology. New York, USA: ACM Press, 2022: 90-96.
[30] 王捷, 葛丽娜, 张桂芬. 区块链的激励机制权益证明共识算法改进方案[J]. 郑州大学学报(工学版), 2023, 44(5): 62-68.
WANG J, GE L N, ZHANG G F. Improvement scheme for the proof of stake consensus of blockchain incentive mechanism[J]. Journal of Zhengzhou University (Engineering Science), 2023, 44(5): 62-68. (in Chinese)

编辑 薛晋栋