文章编号:1671-6833(2023)05-0062-07

区块链的激励机制权益证明共识算法改进方案

王 捷[1,2], 葛丽娜[1,2], 张桂芬[1]

(1.广西民族大学 人工智能学院,广西 南宁 530006; 2.广西民族大学 网络通信工程重点实验室,广西 南宁 530006)

摘 要: 针对权益证明 PoS 出块奖励分配不合理这一问题,提出了一种基于激励机制的权益证明共识算法(Incentive-PoS)。首先,对研究问题进行描述,即 PoS 决定了持币更多的节点获得记账权的概率更大,并且出块奖励由出块者独占;其次,为解决奖励分配的问题,提出基于激励机制的 PoS 共识算法 Incentive-PoS,利用博弈论中的沙普利原理对出块奖励进行再分配,信用度高、积极参与共识的节点都能得到分红,小节点获得收益的可能性变大;最后,对改进算法进行模拟实验与结果分析,相比于原算法,改进方案在分配收益上表现更加合理,提升了获得分红的节点数量、缩小了节点的贫富差距、提高了共识积极性,并且在吞吐量、时延、安全性方面都明显提升。Incentive-PoS 算法有利于改善区块链中因财富差距过大而产生的分层现象,进一步促进了区块链网络的健康运行和发展。

关键词: 区块链; 权益证明共识算法; 激励机制; 沙普利值; 时间戳

中图分类号: TP309.7 **文献标志码**: A **doi**:10.13705/j.issn.1671-6833.2023.02.013

区块链作为比特币的核心技术,起源于 2008 年 Nakamoto 发表的一篇文章[1]。Nakamoto 在文章中提出了一些新的概念:区块、区块链、时间戳(timestamp)等。这篇文章标志着比特币的诞生,同时也向人们展示了区块链这一新技术。区块链因为具有去中心化、可追溯、无法篡改、高安全性等特点,现已经被应用于许多场景中,如金融服务、物联网、医疗等领域[2-4]。

共识机制作为分布式系统中的一个研究热点,区块链技术如果要在未来得到更广泛的应用,就必须研究共识机制。工作量证明(proof-of-work, PoW)[5]源于 Dwork 等[6]对防范垃圾邮件问题进行的研究,比特币采用 PoW 是为了抵抗女巫攻击。PoW 依赖节点算力,导致算力资源的大量浪费、吞吐量低等问题。权益证明(proof-of-stake, PoS)于 2011 年首次被提出[7],在 2012 年发布的点点币(peercoin, PPC)中首次实现。与 PoW 共识算法的算力比拼不同,PoS 的记账权取决于节点的币龄大小(币龄由持币数量与持币时间之积表示)。根据币龄权值的大小降低计算机 Hash 计算的难度,这有效缓解了工作量证明的算力浪费,缩短了共识时间,提高了共识的效率。由于权益证明中权益大的节点获得记账权的概率更高,因此有可能出现权益集中的现象,从而导致“富者越富有,穷人更贫穷”的一家独大的局面,区块链去中心化的特点也将被弱化,共识网络有失公允。

随着共识算法不断改进和优化,性能也在逐渐提高,但是目前的 PoW、PoS 等共识算法对于成功挖矿后获得的奖励没有明确的分配方案,都是由出块者独自占有。PoW 是单纯的算力比拼,出块奖励将全部归出块者所有;PoS 可以看作是币龄的比拼,出块奖励也全部归出块者所有,并且币龄更大者获得记账权且成功出块的概率也更大。对于 PoW、PoS 而言,如果区块链网络中某个节点拥有超过全网一半的算力或币龄,这个节点同样可以通过 51%攻击或利用分叉对整个区块链进行操控,从而获取更多收益。

因此,针对 PoS 出块奖励分配不合理这一问题,提出了基于激励机制的权益证明共识算法(proof of stake based on incentive, Incentive-PoS)。对于积极参与共识、为了挖矿付出努力的节点赋予相应的收益奖励,从而激励小节点积极参与共识。利用博弈论中的沙普利原理对出块奖励进行再次分配,促进更多的小节点积极参与共识,以改善区块链中因财

收稿日期:2022-08-10;**修订日期**:2022-10-13

基金项目:国家自然科学基金资助项目(61862007); 广西壮族自治区自然科学基金资助项目(2020GXNSFBA297103)

通信作者:葛丽娜(1969—),女,广西环江人,广西民族大学教授,博士,主要从事信息安全、物联网和智能计算方面的研究,E-mail:66436539@qq.com。

引用本文: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.)

富差距过大而产生的分层现象。

1　相关研究

基于经典共识算法的改进是区块链技术研究的重点之一。因此,许多研究者对共识算法进行了研究和改进。

Ouroboros 用奖励机制鼓励权益持有者保持在线,激励节点加入区块链以驱动 PoS 共识过程,使得链上诚实节点的行为近似纳什均衡[8],有效地防止区块截留、自私挖矿等攻击。付瑶瑶等[9]提出了一种基于奖励机制和信用机制的 DPoS 改进方案,奖励机制对收益进行再分配,惩罚结合信用机制加大了恶意节点成为代表节点的难度。Hu 等[10]提出了一种基于声誉的 DPoS 共识算法,通过评估节点行为,选择网络中的高质量节点作为共识节点,用激励方法提高节点参与投票的积极性,降低安全风险。康奈尔大学的研究者提出的 Sleepy Consensus 在仅有少数节点在线并参与共识过程的情况下,只需要在线诚实节点的数量超过故障节点的数量即可保证安全性和鲁棒性[11]。Casper 是以太坊在 Serenity 阶段使用的协议,于 2015 年被提出[12],它是一种改进的 PoS 机制,也是基于保证金的经济共识协议(security-deposit based economic consensus protocol)。行动证明 PoA(proof of activity)结合了 PoW 和 PoS,是比特币协议的扩展,它将交易奖励与其他权益持有者、产生空块头的矿工共享[13]。CoA (chains of ativity)[14]沿用 PoA 的思想对 PoS 机制进行了改进,其执行过程类似于一个线上抽奖程序,所有权益持有者遵循协议进行线上抽奖,在一定程度上克服了 PoS 的分叉问题。为防止节点囤币,PoSV 将 PoS 中币龄和时间的线性函数修改为指数式衰减函数,币龄的增长率随时间减少最后趋于 0,新币的币龄比老币增长更快,直到达到上限阈值。燃烧证明(proof of burn,PoB)通过烧毁代币竞争生产新区块的权利,随着时间的推移,节点在系统中所持的份额可能会减少,以此驱动节点燃烧代币获取更多的挖矿机会。PoWaS[15]结合了 PoS 和 PoW,降低哈希计算难度,设置最大难度值、有效持币时间和币龄上限,根据节点行为调节信用值,强化信用值对记账权竞争的影响。Algorand 结合 PoS、BFT 和 VRF,实现了同步网络的快速共识,有效防止了验证权力集中在某些用户手中,去中心化程度高[16]。LaKSA 通过轻量级的委员会投票将节点之间的交互最小化,从而产生比竞争系统更简单、更健壮、更具可扩展性的提案,还减轻了高奖励方差和长确认时间。LaKSA 是基于链的 PoS,专用于但不限于加密货币[17]。Wang 等[18]通过向几何奖励函数添加随机分布来定制新的奖励函数,与其他函数相比,此函数权衡了公平性和激励兼容性,并且其可退出性是最佳的。

2　Incentive-PoS 共识算法设计

共识过程中各节点共同参与并维持一定的动态均衡,他们之间的关系既有竞争又有合作。而博弈论研究的正是个体之间竞争与合作的关系,因此共识过程中各节点之间的关系与博弈论天然契合。运用博弈论的方法构造激励机制,通过数学量化激励,以协调共识过程中各个节点的收入分配,以激励节点积极参与共识。

沙普利值(Shapley value)是博弈论中用来分配收益的一种方法,能够帮助联盟中合作博弈的参与者(即局中人)根据每一位参与者的边际贡献来分配收益。参与者能否获得收益,在于这位参与者对联盟或系统产生的边际效益[19]。沙普利值利用边际效益的概念来衡量合作博弈中每个参与者的价值。

共识算法规定了区块链中各节点之间的约束关系,本算法的主要思想在于:出块节点向全网进行广播,其他节点对新广播的区块合法性进行验证,如果验证合法,则此区块是有效区块,被添加到区块链上。出块节点获得记账权后,出块节点和参与验证的节点之间组成一个联盟节点集合,通过沙普利值的计算方式,计算联盟节点集合中节点的分红,最后分发出块分红。根据联盟节点集合中各节点在共识过程中具体做出的贡献获得一定比例的收益分红。

基于沙普利值的收益分配方案如下所述。

(1)首先,根据信用度评估模型提取出信用度排名前 10%的节点,将这些信用度良好的节点构成一个集合 N,对其进行编号:1,2,…,n,在算法中将之称为信用节点集合。

$$N = \{node_1, node_2, \cdots, node_n\}。\tag{1}$$

(2)对于一次共识博弈,所有节点进行记账权竞争和有效区块验证,一个节点挖矿成功后,会向全网广播,其余节点会对广播的新区块进行合法性验证。此时,提取出对区块及时进行验证的前 10%的节点,将这些及时响应验证的节点构成一个集合 M,对其进行编号:1,2,…,m,在算法中将之称为及时验证集合。

$$M = \{node_1, node_2, \cdots, node_m\}。\tag{2}$$

(3)将信用节点集合 N 与及时验证集合 M 取

交集,得到一个新集合 W。

(4)定义价值函数。函数 $v:2^N \mapsto \mathbf{R}$ 是为每个集合(W 的一个子集称为一个联盟)$Z \subseteq W$ 定义了价值函数 $v(Z)$,并且规定 $v(\phi)=0$。

(5)用 $W \subseteq 2^N$ 表示信用节点的联盟。因此,对于任意属于 W 的联盟 Z,价值函数 $v(Z)$ 定义为

$$v(Z)=\begin{cases}1, & Z \notin W;\\ 0, & Z \in W。\end{cases} \tag{3}$$

(6)在联盟节点集合中,每个节点的沙普利值表示为

$$\phi_i(N,v)=\frac{1}{|N|!}\sum_{Z\subseteq N\setminus\{i\}}|Z|!\,(|N|-|Z|-1)!\cdot[v(Z\cup\{i\})-v(Z)]。 \tag{4}$$

(7)引入时间因素后,将响应时间作为影响收益分配的一个元素,节点沙普利值计算公式为

$$\varphi_i^T(N,V)=\frac{\varphi_i(N,V)}{T_e-T_s}; \tag{5}$$

$$T=T_e-T_s; \tag{6}$$

$$\varphi_i^T(N,V)=\frac{\varphi_i(N,V)}{T}。 \tag{7}$$

式中:T_s 表示节点挖矿成功后,将新区块打包进行全网广播的起始时间;T_e 表示在线节点对新区块信息验证其合法性的结束时间;T_e-T_s 表示发起广播至验证结束所花费的时间。令 $T=T_e-T_s$,T 的值越小,节点验证区块的时间越迅速,说明该节点验证的积极性越高。因此,分式中的分母越小,节点的沙普利值就越大,该节点验证所得的奖励将越高。将式(6)代入式(5),得到式(7)。

(8)拥有记账权的节点通过打包区块获得的出块奖励记为 R,根据节点的信用度对区块奖励进行再分配,则联盟中的节点 i 获得的最终收益为

$$R_i=R\cdot\varphi_i^T(N,V)\cdot\frac{credit_i}{\sum_{j=1}^{Num\_W}credit_i}。 \tag{8}$$

3 实验结果与分析

实验系统配置为 AMD R7 5800H CPU 3.20 GHz 处理器,16 GB 内存,64 位的 Ubuntu 21.04,用 Golang1.16.2 在 Fabric 环境下实现 PoS 共识算法和 Incentive-PoS 共识算法。

基于激励机制的权益证明共识算法 Incentive-PoS 旨在解决 PoS 共识算法收益分配不合理的问题。为了验证改进算法的效果,从 3 个方面进行分析:一是出块奖励的分配,主要的分析内容为获得出块奖励分红的节点数目以及每个节点的经济状况;二是节点参与共识的积极性,主要通过参与共识的节点数量来反映;三是为分析改进算法的性能,将从吞吐量、出块时间与安全性对改进算法进行分析。

3.1 收益分配合理化分析

为分析 Incentive-PoS 的收益分配情况,对比分析了算法改进前后获得出块奖励分红的节点数目以及各个节点的经济状况,经济状况通过节点的账户余额反映。

3.1.1 分红节点数

在相同的实验配置与环境下,分别模拟了参与共识在节点总数不同的情况下 Incentive-PoS 与 PoS 的表现。算法改进前后获得分红的节点数量如图 1 所示。实验结果表明:PoS 获得出块奖励的节点数量固定为 1,改进算法随着参与共识的节点数量的增加获得分红的节点也越多。其原因在于 PoS 的出块奖励为出块者独自享有,改进算法基于激励机制引入沙普利原理为信用良好、及时参与验证的节点进行出块奖励分红,增加了获得分红的节点数量。这与算法设计的目的相吻合,收益的分配相比于原算法更合理,获得收益的节点更多,付出努力的节点也收获了相应的分红。

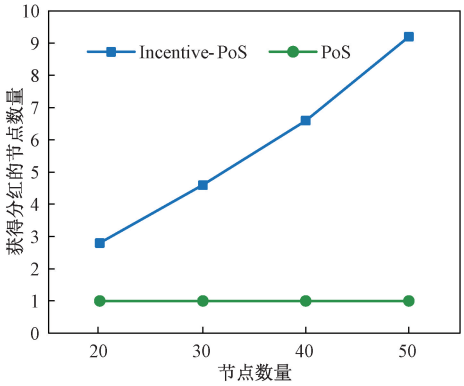

图 1 获得分红的节点数

Figure 1 Number of nodes in the dividend

3.1.2 节点经济状况

收益分配合理化分析的另一方面是节点的经济状况,经济状况主要通过节点账户所存储的代币数量反映。对比算法改进前后各个节点的经济状况,可以分析出块奖励的分配情况,同时还能分析节点的财产集中化程度。

保持实验配置环境不变,对 Incentive-PoS 进行了模拟实验。实验选取了相同时间段下 20 个节点的账户财产对比情况,如图 2 所示。从图 2 可以看出,PoS、Credit-PoS[20]、Incentive-PoS 3 种共识算法中各节点之间经济的差距情况:PoS>Credit-PoS>Incentive-PoS。PoS 中节点经济差距悬殊,Credit-PoS

相比于 PoS 经济差距较小,Incentive-PoS 的折线图在 3 种算法中波动的幅度最小,因而显示出经济的差距更小,在奖励的分配上表现出公平性并且有助于区块链网络中节点权益的分散化。

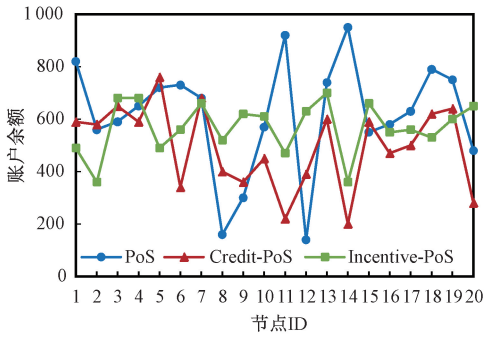

图 2　20 个节点的账户余额

Figure 2　Account balance of 20 nodes

引入基尼系数对节点的奖励分配进行进一步分析,在 PoS、Credit-PoS、Incentive-PoS 3 种共识算法下区块链中节点财富状况所对应的基尼系数如表 1 所示,表中系数根据图 2 中数据计算得出。

表 1　3 种算法基尼系数对比

Table 1　Gini coefficient comparison of three algorithms

算法	基尼系数
Incentive-PoS	0.251
Credit-PoS	0.304
PoS	0.506

从结果可以看到,3 种共识算法下的基尼系数大小为:Incentive-PoS<Credit-PoS<PoS,即 Incentive-PoS 收益的分配表现最公平。对照基尼系数标准表 2 可以得出,Credit-PoS 将 PoS 收益分配调节得比较合理,Incentive-PoS 在 Credit-PoS 的基础上将收益分配调整至较于平均。Incentive-PoS 下各节点的收益分配在分散权益和防止一家独大的问题上效果显著,但是从另一方面来看,收入分配如果过于平均则不利于促进经济的健康和谐发展。

表 2　基尼系数标准

Table 2　Gini coefficient standard

基尼系数	收入分配情况
[0,0.2)	过于平均
[0.2,0.3)	较为平均
[0.3,0.4)	比较合理
[0.4,0.5)	差距过大
[0.5,1.0]	差距悬殊

3.2　共识积极性分析

Incentive-PoS 激励机制的目的在于利用收益分红激励更多节点参与到共识中,为了验证激励机制的激励作用,通过实验分析了 PoS、Credit-PoS、Incentive-PoS 3 种共识算法中节点参与共识的积极性。实验在各节点初始币龄相同的情况下,模拟了 100 个节点的 70 轮共识。对各轮次中参与共识的节点进行了统计并计算参与共识的节点的比例,实验结果如图 3 所示。

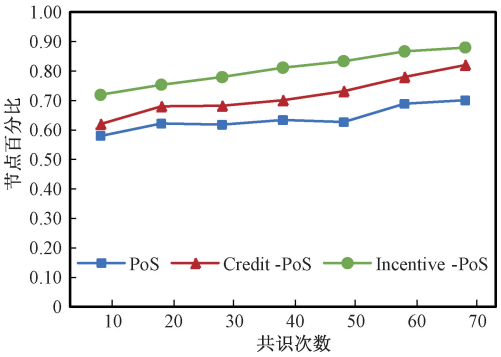

图 3　参与共识的节点比例

Figure 3　Proportion of nodes participating in consensus

从图 3 可以看出,3 个算法中参与共识的节点比例均呈现上升趋势,3 种共识算法下参与共识的节点比例的平均值大小为 Incentive-PoS>Credit-PoS>PoS。PoS 在多轮共识中,节点的参与度在 58%~70%内,平均节点参与比例约为 65%;Credit-PoS 在多轮共识中节点的参与度在 62%~82%之间,平均节点参与比例为 73%;Incentive-PoS 在多轮共识中节点的参与度在 72%~88%之间,平均节点参与比例为 83%。究其原因可知,Credit-PoS 将 PoS 的币龄比拼转换为信用比拼,在一定程度上激发了节点参与共识的积极性;Incentive-PoS 的激励机制利用沙普利原理对信用节点和及时验证节点进行收益分红的奖励方式,在激励节点参与共识的积极性上得到了进一步的提升。由此可以得出,改进方案 Incentive-PoS 能够有效地提高节点参与共识的积极性。

3.3　性能分析

3.3.1　吞吐量分析

在测试吞吐量性能时,保持实验环境不变,设置节点数量为 10 至 50 个依次递增,在规定时间内对共识算法完成的交易数据进行记录,对比分析 Incentive-PoS 与 PoS、PoW、PBFT、DPoS 的吞吐量。实验结果如图 4 所示。

首先分析不同共识节点数量下的吞吐量情况。节点数为 10 时的吞吐量大小关系为 PBFT>DPoS>Incentive-PoS>PoS>PoW;在节点数为 20、30、40、50 的情况下,吞吐量大小关系均为 Incentive-PoS>PBFT>DPoS>PoS>PoW。由此可以看出,在共识节点数量增多的情况下,Incentive-PoS 在吞吐量上更

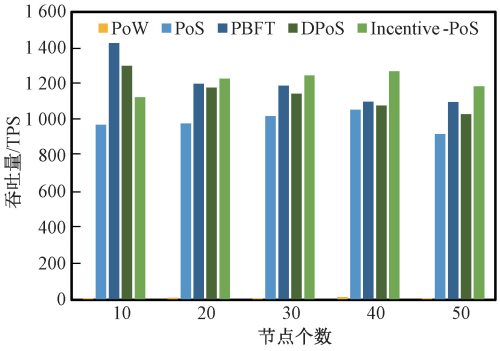

图 4 吞吐量对比图

Figure 4 Throughput comparison chart

具稳定性。

其次分析 5 种共识算法的吞吐量平均值。表 3 为实验中共识算法 5 组数据的吞吐量平均值。从表 3 中可以得知,这几种共识算法的平均值大小关系:Incentive-PoS>PBFT>DPoS>PoS>PoW ,Incentive-PoS 的吞吐量在这几个算法中表现最优。其主要原因在于改进算法的激励机制提高了节点的积极验证过程,这在一定程度上提高了共识的效率。综合以上对比分析,改进方案在合理分配出块奖励与提高节点参与共识积极性的同时,在吞吐量的性能上也有所提升。

表 3 不同算法平均吞吐量

Table 3 Average throughput of Different algorithms

共识算法	平均吞吐量/TPS
PoW	9.8
PoS	990.2
DPoS	1 147.0
PBFT	1 203.4
Incentive-PoS	1 211.6

3.3.2 时延分析

实验模拟了 Incentive-PoS 与 PoS、PoW、DPoS 在相同条件下的 100 次出块情况,并统计其出块时间以分析时延。实验结果如图 5、表 4 所示。从实验结果可以得出每个算法的出块时间:PoW ≫ PoS >Incentive-PoS>DPoS。其中 PoW 与 PoS 算法的出块时间总体看来波动幅度较大、峰值较多,PoW 出块时间达到了 10 min 以上,PoS 的出块时间最高也达到了分钟级。Incentive-PoS 与 DPoS 可以达到秒级,DPoS 时延最低,Incentive-PoS 时延较 DPoS 要高一些。Incentive-PoS 的表现较 PoW 与 PoS 而言峰值少、波动幅度小,且算法的出块时间更规律,显著提高了时延性能的稳定性。从表 4 中的平均出块时间可以看出,Incentive-PoS 达到了秒级,较 PoW 与 PoS 实现了分钟级到秒级的提升。

综合分析可以得出,Incentive-PoS 在时延的模拟实验中虽表现为次优,但是在原算法 PoS 的基础上实现了量级的提升,改进算法在时间开销上具有明显优势。改进方案在延时上相较于原算法 PoS 性能表现更优。

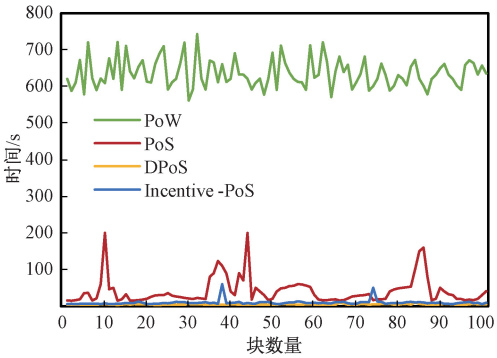

图 5 各算法出块时间

Figure 5 Block time each algorithm

表 4 不同算法平均出块时间

Table 4 Average block time of Different algorithms

共识算法	平均出块时间/s
PoW	635.868
PoS	41.358
DPoS	4.529
Incentive-PoS	10.024

3.3.3 安全性

考虑到现实网络中存在非诚实节点,实验模拟了初始状态下 100 个共识节点中存在 20 个恶意节点的情况。进行 50 轮共识,并统计系统中恶意节点的数量,以验证改进算法的安全性。如图 6 所示,对比分析了改进算法与 PoS、基于信用机制的 DPoS 改进方案 Credit-DPoS[21]、基于信誉投票的 PBFT 改进方案 Credit-PBFT[22] 在相同条件下剔除恶意节点的情况。

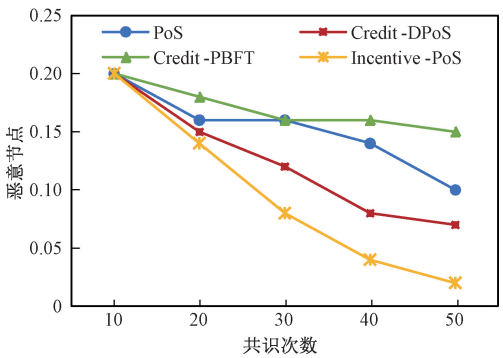

图 6 不同算法恶意节点对比

Figure 6 Comparison of malicious nodes of Different algorithms

横向分析:4 条线段都呈现下降的趋势,随着共识轮数的增加,预设的恶意节点数量都有所减少,这

意味着 4 种改进方案都能够在共识过程中剔除恶意节点;纵向分析:在对比方案中,Incentive-PoS 算法中恶意节点数始终小于其他方案,并且恶意节点的剔除速度为 Incentive-PoS>Credit-DPoS>PoS>Credit-PBFT。

综上,随着共识轮数的增加,Incentive-PoS 改进算法在剔除恶意节点的数量与效率上均优于其他对比方案。Incentive-PoS 算法可以快速高效地剔除恶意节点,具有安全性。

4　结论

为了解决 PoS 出块奖励分配不合理这一问题,提出了基于激励机制的 PoS 共识算法 Incentive-PoS。引入博弈论中的沙普利原理对出块奖励进行再分配,使积极参与共识的节点以及诚实节点也能够获得一定的出块奖励分红,让区块链网络中的小节点也有机会获得收益,以此激励小节点积极参与共识,激励更多的节点成为诚实节点。实验结果显示:Incentive-PoS 相比于原算法在分配收益上的表现更加合理,并且能够激励节点参与共识的积极性。在吞吐量、时延、安全性方面,较于原算法都明显提升。这有利于改善区块链中因财富差距过大而产生的分层现象,进一步促进了区块链网络的健康运行和发展。

Incentive-PoS 的改进方案为区块链共识算法的改进提供了新的研究思路,对出块奖励进行了合理的分配,但在时延上对比 DPoS 仍存在一定的差距,接下来的工作中还需要不断优化算法,继续提升算法的性能。此外,还需研究如何使得节点的权益分配可以更好地达到纳什均衡。

参考文献:

[1] NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system[EB/OL]. (2009-03-01)[2022-06-13]. http://bitcoin.org/bitcoin.pdf.

[2] ZHENG Z B, XIE S A, DAI H N, et al. An overview of blockchain technology: architecture, consensus, and future trends[C]//2017 IEEE International Congress on Big Data (BigData Congress). Piscataway: IEEE, 2017: 557-564.

[3] 李永强, 刘兆伟. 基于区块链的车联网安全信息共享机制设计[J]. 郑州大学学报(工学版), 2022, 43(1): 103-110.
LI Y Q, LIU Z W. Blockchain-based secure data sharing mechanism design in the vehicular networks[J]. Journal of Zhengzhou University (Engineering Science), 2022, 43(1): 103-110.

[4] YUAN Y, WANG F Y. Blockchain and cryptocurrencies: model, techniques, and applications[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2018, 48(9): 1421-1428.

[5] DWORK C, NAOR M. Pricing via processing or combatting junk mail[C]//12th Annual International Cryptology Conference. Berlin: Springer, 2007: 139-147.

[6] DOUCEUR J R. The sybil attack[C]//International Workshop on Peer-to-Peer Systems. Berlin: Springer, 2002: 251-260.

[7] KING S, NADAL S. Ppcoin: peer-to-peer crypto-currency with proof-of-stake[EB/OL]. (2012-08-19)[2022-06-12]. https://people.cs.georgetown.edu/~clay/classes/fall2017/835/papers/peercoin-paper.pdf.

[8] 袁勇, 倪晓春, 曾帅, 等. 区块链共识算法的发展现状与展望[J]. 自动化学报, 2018, 44(11): 2011-2022.
YUAN Y, NI X C, ZENG S, et al. Blockchain consensus algorithms: the state of the art and future trends[J]. Acta Automatica Sinica, 2018, 44(11): 2011-2022.

[9] 付瑶瑶, 李盛恩. 授权股份证明共识机制的改进方案[J]. 计算机工程与应用, 2020, 56(19): 48-54.
FU Y Y, LI S G. Improved scheme of delegated proof of stake consensus mechanism[J]. Computer Engineering and Applications, 2020, 56(19): 48-54.

[10] HU Q, YAN B W, HAN Y B, et al. An improved delegated proof of stake consensus algorithm[J]. Procedia Computer Science, 2021, 187: 341-346.

[11] PASS R, SHI E. The sleepy model of consensus[C]//International Conference on the Theory and Application of Cryptology and Information Security. Cham: Springer, 2017: 380-409.

[12] ZAMFIR V. Introducing casper "the friendly ghost"[EB/OL]. (2015-08-01)[2022-06-13]. https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost.

[13] BENTOV I, LEE C, MIZRAHI A, et al. Proof of activity[J]. ACM SIGMETRICS Performance Evaluation Review, 2014, 42(3): 34-37.

[14] BENTOV I, GABIZON A, MIZRAHI A. Cryptocurrencies without proof of work[M]//Financial Cryptography and Data Security. Berlin: Springer Heidelberg, 2016: 142-157.

[15] 刘怡然, 柯俊明, 蒋瀚, 等. 基于沙普利值计算的区块链中 PoS 共识机制的改进[J]. 计算机研究与发展, 2018, 55(10): 2208-2218.
LIU Y R, KE J M, JIANG H, et al. Improvement of the PoS consensus mechanism in blockchain based on Shapley value[J]. Journal of Computer Research and Develop-

ment, 2018, 55(10): 2208-2218.
[16] GILAD Y, HEMO R, MICALI S, et al. Algorand: scaling Byzantine agreements for cryptocurrencies[C]//Proceedings of the 26th Symposium on Operating Systems Principles. New York: ACM, 2017: 51-68.
[17] REIJSBERGEN D, SZALACHOWSKI P, KE J M, et al. LaKSA: a probabilistic proof-of-stake protocol[C]//Proceedings 2021 Network and Distributed System Security Symposium. Reston: Internet Society, 2021.
[18] 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.
[19] 赵越. 区块链混合共识算法研究[D]. 哈尔滨: 哈尔滨工业大学, 2019.
ZHAO Y. Research on blockchain consensus algorithm[D]. Harbin: Harbin Institute of Technology, 2019.
[20] WANG J, GE L N. Consensus algorithm of proof-of-stake based on credit model[C]//The 2022 4th International Conference on Blockchain Technology. New York: ACM, 2022: 90-96.
[21] 黄嘉成, 许新华, 王世纯. 委托权益证明共识机制的改进方案[J]. 计算机应用, 2019, 39(7): 2162-2167.
HUANG J C, XU X H, WANG S C. Improved scheme of delegated proof of stake consensus mechanism[J]. Journal of Computer Applications, 2019, 39(7): 2162-2167.
[22] 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.

Improvement Scheme for the Proof of Stake Consensus of Blockchain Incentive Mechanism

WANG Jie[1,2], GE Lina[1,2], ZHANG Guifen[1]

(1. Department of Artificial Intelligence, Guangxi Minzu University, Nanning 530006, China; 2. Key Laboratory of Network Communication Engineering, Guangxi Minzu University, Nanning 530006, China)

Abstract: To solve the problem of unreasonable distribution of PoS block rewards, a proof of stake based on incentive (Incentive-PoS) consensus algorithm was proposed. Firstly, the research problem was described. A PoS determined that nodes with more coins have a greater chance of obtaining accounting rights, and the block reward was exclusively owned by the block producer. Secondly, in order to solve the problem of reward distribution, a PoS consensus algorithm based on incentive mechanism was proposed, Shapley's principle in game theory was uesd to redistribute block rewards. Nodes with high credibility and active participation in consensus would receive dividends, and made small nodes more likely to obtain benefits. Finally, the simulation experiment and result analysis of the improved algorithm were carried out. Compared with the original algorithm, the improved scheme had a more reasonable performance in the distribution of income, and increased the number of nodes receiving dividends, reduced the gap between the rich and the poor, and improved the enthusiasm of consensus. And the throughput, latency, and security were significantly improved. It was beneficial to improve the stratification phenomenon caused by the excessive wealth gap in the blockchain, and could further promote the healthy operation and development of the blockchain network.

Keywords: blockchain; proof of stake; incentive mechanism; Shapley value; times-tamp