计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.190400013

基于“奖励制度”的 DPoS 共识机制改进

陈梦蓉[1] 林 英[1,2] 兰 微[1] 单今朝[1]
1 云南大学软件学院 昆明 650091
2 云南省软件工程重点实验室 昆明 650091
(limchen@mail.ynu.edu.cn)

摘 要 共识机制是区块链技术的核心。授权股权证明(Delegated Proof-of-Stake,DPoS)作为一种共识机制,其中每个节点都能够自主决定其信任的授权节点,从而实现快速共识验证。但 DPoS 机制仍然存在着节点投票不积极以及节点腐败的安全问题。针对这两个问题,文中提出了基于奖励的 DPoS 改进方案,投票奖励用以激励节点积极参与投票,举报奖励用以激励节点积极举报贿赂节点。Matlab 仿真结果表明,投票奖励方法的引入提高了节点投票的积极性。与原始 DPoS 共识机制下投票节点数占比 45%～50%相比,两种投票奖励方法使得参与投票节点数占比分别增加至 65%～70%以及 55%～60%。相比原始 DPoS 共识机制下不接受贿赂节点占比会随着恶意节点贿赂力度的加大而不断减少的情况,举报奖励方法的引入使得选择举报节点的占比出现了明显增加,在投票轮数为 20 的情况下,选择举报节点的总占比可以增至 54%。实验结果表明,奖励制度的引入不但能够提高节点投票的积极性,而且增强了普通节点对恶意节点的贿赂抵抗性,使恶意节点成“代理人节点”的概率变小,保障了网络安全性。

关键词:区块链;共识机制;授权股权证明;奖励机制;算法改进;博弈论
中图法分类号 TP309

Improvement of DPoS Consensus Mechanism Based on Positive Incentive

CHEN Meng-rong[1],LIN Ying[1,2],LAN Wei[1] and SHAN Jin-zhao[1]
1 School of Software,Yunnan University,Kunming 650091,China
2 Key Laboratory for Software Engineering of Yunnan Province,Kunming 650091,China

Abstract Consensus mechanism is the key of block chain technology. In the DPoS consensus mechanism,each node can independently determine its trusted authorization nodes,and these authorization nodes will take turns to generate new blocks for rapid consensus verification. But DPoS still has security problems such as inactive voting and node corruption. Aiming at these two problems,this paper proposed an improved DPoS scheme based on reward incentive. The evoting rewardr is used to encourage nodes to actively participate in the process of voting and the ereporting rewardr is used to encourage common nodes to report bribery nodes. The Matlab simulation experiments show that the introduction of voting reward improves the voting enthusiasm of nodes. Compared with the original DPoS consensus mechanism,in which the number of voting nodes accounts for 45% to 50%,the introduction of two different voting reward methods increases the number of voting nodes to 65% to 70% and 55% to 60% respectively. Compared with the original DPoS consensus mechanism,in which the proportion of nodes that do not accept bribes will decrease as the bribery of malicious nodes increases,the introduction of the reporting reward method makes the proportion of choosing reporting nodes increase significantly,and the proportion of choosing reporting nodes can increase to 54% when the number of voting rounds is 20. The experiment results show that the improved DPoS mechanism can not only make more nodes vote,but also enhance the bribery resistance of the common nodes,so that the probability of malicious nodes becoming the “trustee” becomes smaller,thus ensuring the security of the network.

到稿日期:2019-04-02 返修日期:2019-09-02 本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:国家自然科学基金项目(61462092,61379032,61662085);云南省软件工程重点实验室项目(2017SE102);云南大学数据驱动的软件工程省科技创新团队项目(2017HC012);云南省教育厅科学研究基金项目(2019Y0009);云南大学研究生科研创新基金项目(2018Z087);云南大学大学生科研创新创业训练(科技创新类)项目(201804066)
This work was supported by the National Natural Science Foundation of China (61462092,61379032,61662085),Key Laboratory Project of Software Engineering in Yunnan Province(2017SE102),Yunnan University Data-driven Software Engineering Provincial Science and Technology Innovation Team Project(2017HC012),Scientific Research Foundation Project of Yunnan Education Department(2019Y0009),Yunnan University Graduate Research Innovation Fund Project(2018Z087),Scientific Research Innovation and Entrepreneurship Training (Science and Technology Innovation) for Yunnan University Students(201804066).
通信作者:林英(linying@ynu.edu.cn)

Keywords Blockchain, Consensus mechanism, Delegated proof-of-stake, Incentive mechanism, Algorithm improvement, Game theory

1 引言

近年来,区块链的运用涉及智能合约、医疗、金融、物联网、交通等多个领域[1-5],如何在决策权高度分散的去中心化系统中使得各节点高效地对区块数据的有效性及一致性达成共识一直是区块链技术研究的重点之一[6]。工作量证明(Proof-of-Work,PoW)、权益证明(Proof-of-Stake,PoS)以及DPoS[7]等不同共识机制的相继提出,解决了区块链中由谁来记账、长期存在的拜占庭以及如何维护账本统一的问题[8]。

PoW共识机制的核心思想是各个节点通过算力竞争来解决一个HASH难题,从而保证网络分布式记账的一致性以及共识的安全性[9]。比特币区块链系统的安全性和不可篡改性就是由高度依赖节点算力的PoW共识机制所保证的[6],但这也暴露了PoW共识机制需要计算机拥有强大算力的缺点。Gramol[10]列出了PoW共识机制中存在的主要漏洞,并详细阐述了未准确理解和使用PoW机制而产生的一些潜在威胁:风险和收益的博弈必然会导致联合挖矿的问题,所以在PoW共识机制下,如果不是首个算出合理HASH值的节点,那么即使付出了很大的经济成本计算HASH值,也仍然得不到回报。

针对PoW存在的问题,文献[11]提到一位数字货币爱好者于2011年在Bitcointalk论坛中首次提出了PoS共识机制,该机制被证明具有很好的可行性和可扩展性[12]。PoS的本质是采用权益证明来代替PoW中的基于算力的工作量证明,由系统中具有最高权益而非最高算力的节点获得区块记账权[13]。这里的最高权益通常用币龄来表现,币龄越大则可以优先获得记账权生产区块。PoS在一定程度上缩短了达成共识的时间,减少了PoW机制的资源浪费。但PoS共识机制也存在一些缺点:会出现"Nothing of Stake"[14]的安全性问题,如果大部分资源都掌握在富人手上,按照币龄的大小来决定记账权则会出现"富人越富,穷人越穷"的局面,从而使得网络共识的公正性遭到破坏[15]。

DPoS作为PoS的演化版本,其记账权由节点投票产生,普通节点不但可以投票给相对可信的代表作为区块生产者,也可以选择在下一轮投票环节中通过不投票而解雇区块生产者[13]。在DPoS共识机制中,由于每个节点都能够自主决定其信任的授权节点,且由这些授权节点轮流记账生成新区块,因此大幅减少了参与验证和记账的节点数量,从而实现了快速共识验证。但DPoS也存在着如下风险:普通节点不积极参与投票,因为选举代表需要消耗大量的时间和算力;任何一个持币节点都可以参与到投票和竞选代表这两个过程中,每个节点投票的权重和持币量成正比,因此可能存在恶意节点贿赂权重较大的节点给自己投票的潜在风险,从而产生腐败贿赂的现象,并且如果恶意节点在生产链中只是为了获得更多的利益而没有能力去生产区块,则将会导致整个区块链的生产能力下降,所有节点的利益都将受到损害。

本文旨在深入了解DPoS机制,针对其存在的这两个问题进行改进。主要贡献在于:

(1)设计了两种投票奖励机制,并且讨论了不同投票奖励机制适用于不同场景,以便激励节点积极参与投票;

(2)将博弈论作为分析工具,在博弈策略下建立"举报"机制,对举报恶意节点的行为实施相应奖励并且对恶意节点进行相应处罚,从而有效抑制节点腐败的问题;

(3)通过实验仿真,有效验证了本文方法的可行性。

本文第2节介绍了基于奖励的共识机制改进的相关工作;第3节介绍了基于奖励制度的DPoS改进与实现策略;第4节进行实验和分析;最后总结全文。

2 相关工作

基于奖惩激励机制的共识机制改进,是区块链技术研究的重点之一。文献[16]提出区块链共识机制的未来研究趋势将侧重于共识算法的性能评估、激励机制的适配优化和新型区块链下共识算法的改进;并且着重强调了激励机制是保障区块链系统健康稳定运行的关键,迫切需要未来研究的跟进。

共识机制中的奖惩激励机制方案,最早由Chiu等提出[17]。其基于PoW共识机制设计了一个节点,通过相互竞争来加快区块链更新以获得奖励的模型,其中节点更新区块的速度越快,系统所给奖励也越多,而对于那些试图篡改所有权记录的节点,一经发现就对其进行双倍的惩罚。这个机制可以大大提高PoW共识机制下节点生产区块的效率,但是PoW共识机制本身的强大算力要求,限制了该机制的应用。文献[18]指出区块链中的一个开放性问题便是奖励机制的改进,并以PoW和PoS共识机制为基础,探讨了如何激励诚实节点,使其协议执行力和生产力得到提高,同时保证不能过度激励导致节点中心化。文献[19]指出了PoW共识机制面临的挖矿困境问题,即矿工们为了获得更大的利益而选择对正在挖矿的节点进行区块截留攻击,而当所有矿工都选择这种策略时,会由于没有矿工挖矿而导致整个矿池的收益为零。其对此采用了零行列式策略来对矿工策略选择进行优化,最终达到了激励矿工合作挖矿的目的。文献[20]提出了现有共识机制存在着对参与生成区块的节点没有一种具体收益分配方案的问题,并以PoS共识机制为例,提出了一种基于博弈论中计算沙普利值的原理设计的激励机制,使参与生产的区块收益更加公平,大幅提高了新加节点获得收益的可能性,以激励节点积极参与区块的生产,从而达到消除系统中心化的目标。文献[21]也指出了低事务吞吐量和可扩展性差是公共区块链共识机制中存在的问题,并且为了解决这些问题建立了一个博弈模型,提出了一种新的激励兼容分享机制,促进了公共区块链内部的合作,也抑制了"搭便车"的现象。

关于DPoS共识机制安全方面的研究,Wang等[22]指出,为了适应实际交易,牺牲部分安全性以换取效率的共识机制十分普遍,DPoS共识机制就是其中的典型代表。文献[23]在分析区块链存在的现有安全威胁时提到了共识机制中的贿赂攻击,明确地指出贿赂攻击除了对工作量证明PoW无效以

外，对其余共识机制都存在风险。文献[24]为了保证车联网中数据共享的安全性和可追溯性，利用 DPoS 共识机制建立了基于区块链的车联网机制，但其指出：DPoS 共识机制由于利用类似于股份投票制度来选出区块生产者，因此会出现候选者节点和权重高的节点共谋的问题，同时恶意节点也会通过贿赂权重高的节点来达到成为区块生产者的目的。该文献提出了基于信誉的投票方案，以确保高信誉和高效率的节点被选为区块生产；并且设置激励机制来激励节点参与投票和选举，防止部分活跃的节点内部串通。文献[25]提出了基于 DPoS 机制的一种新的投票算法，采用改进的基于环的协调器选择算法作为协商一致的算法，从而确保整个过程的分权和公平，防止垄断。但是其提出的协商一致性算法是由整个网络节点选择的块生成器，一旦在网络延迟或者消息还没到达整个网络的情况下就进行选举，整个网络就不可能达成一致的选择。

本文基于文献[26]提出的货币激励能确保大多数共识节点/矿工遵循区块链状态转换规则的观点，对 DPoS 共识机制进行研究与改进；讨论了激励机制和 DPoS 共识机制之间的适配和优化，解决了 DPoS 共识机制中存在的投票不积极的问题。针对文献[27]提出的激励机制对危害区块链安全性的攻击行为没有相应的对策这一问题，本文提出了“举报奖励”这一激励制度，并通过博弈分析来确保选举过程中如果出现腐败和贿赂攻击的威胁，大部分节点将会自发地对这一攻击进行抵御。

3 DPoS 机制的改进

3.1 奖励制度的基本原理

本文定义了两种奖励制度：1)投票奖励制度，用以激励节点积极参与投票，从而解决 DPoS 中绝大多数普通节点不积极参与投票的缺点；2)举报奖励制度，用以激励节点积极举报恶意节点，从而解决 DPoS 中出现恶意节点贿赂其他节点给其投票的腐败现象。奖励可以体现为节点的收益，在不同业务领域的区块链系统中，该收益可以被赋予实际的价值，例如在选举阶段，收益可以作为衡量节点是否具有代表资格的一项权值，或者收益可以折合为一定的数字货币。

(1)奖励制度的设计

基于投票奖励机制的具体流程如图 1 所示。

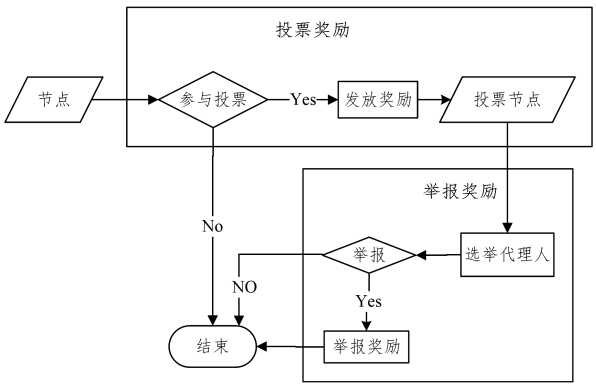

图 1 基于投票奖励的工作流程图

Fig. 1 Work flow chart based on voting reward

本文将 DPoS 共识机制中的投票选举这一过程设计为两个阶段：节点投票奖励阶段和举报奖励阶段。为了解决 90% 以上的节点不参与投票的问题，系统设定：节点只要参与投票，系统就发放奖励，从而正向激励节点积极参加投票。在选举过程中，参与投票的节点如果被恶意节点贿赂并选择了举报，系统就对该节点发放奖励。

(2)基于时间成本的投票奖励制度

投票奖励的改进方案虽然能够正向激励节点积极参与投票，但仍然存在一个问题，即会出现一些节点在没有时间限制的情况下拖延投票的情况。为了提高选举效率，本文提出了基于时间成本的投票奖励方案，具体流程如图 2 所示。仍然将 DPoS 共识机制中的投票选举过程分为投票奖励及举报奖励两个阶段，只是为了缩短时间并提高效率，在节点投票选取代理人的过程中，系统会根据投票参与人数规定一个时间界限。如果节点在时间范围内能完成代理人的选举，则系统发放奖励，且完成的时间越短，全体节点得到的奖励越大；如果超出规定的时间范围，则全体节点都没有奖励，从而正向激励节点积极参加投票。在举报奖励阶段，如果参与投票的节点被恶意节点贿赂并选择了举报，则系统对该节点发放奖励。

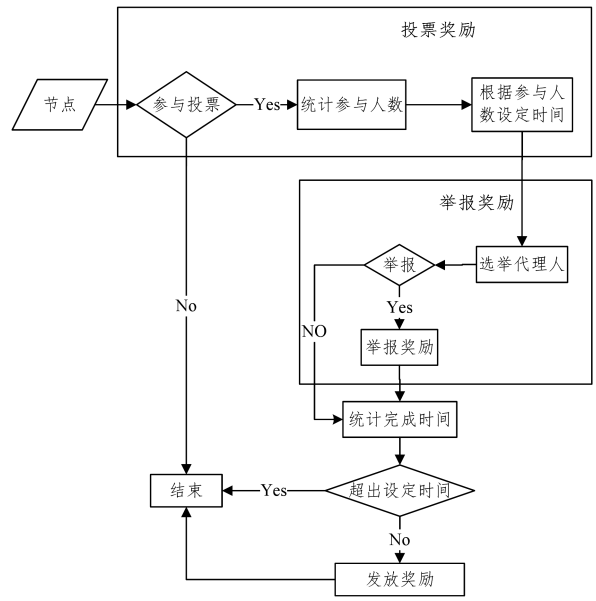

图 2 基于时间成本奖励的工作流程图

Fig. 2 Work flow chart based on time cost reward

3.2 博弈角度下的潜在贿赂主体的决策分析

博弈论主要研究整个博弈中激励结构的相互作用，采用一定的策略以实现自身利益的最大化，它是一种处理合作与竞争的决策手段。运用博弈论来分析区块链中的激励机制是一种必然的方式[28]。本节通过对贿赂主体(竞选代理人节点)和选民节点等利益相关者进行博弈分析，建立相应的收益分析表，以期根据相应的数学分析设计出抵御贿赂攻击的有效奖惩机制。

(1)假设 A 是 DPoS 共识机制中竞选代理人的节点，而 B 是选民节点。A 有进行贿赂(P)和不进行贿赂(Q)两种策略，策略集为$\{P,Q\}$；B 有选择接受贿赂(E)和举报(F)两种策略，策略集为$\{E,F\}$。

(2)假设 r 为 A 贿赂成功所带来的收益；g 为被举报的处罚；m 为 A 正常工作所得的正常收益（我们规定 $m<r<g$）；t 为 B 接受贿赂所得的额外收益；g 为选择举报所得的额外收益。A 和 B 的收益矩阵如表 1 所列（规定被举报节点扣除的收益即为举报节点的奖励收益）。

表 1 收益分析表

Table 1 Income analysis

策略	E	F
P	r,t	$-g,g$
Q	$m,0$	$m,0$

假设 A（竞选代理人节点）采取 P（进行贿赂）策略的节点比例为 X，则采取 Q（不进行贿赂）策略的节点比例为 $1-X$；同理，B（选民节点）采取 E（接受贿赂）策略的节点比例为 Y，则采取 F（举报）策略的节点比例为 $1-Y$。

用 U_p 表示 A（竞选代理人节点）选择 P 策略的期望收益，用 U_Q 表示 A 选择 Q 策略的期望收益，$\bar{U_A}$ 为竞选代理人节点的平均收益，则：

$$U_p=Y\cdot r+(1-Y)(-g)=Y\cdot r+g(Y-1) \tag{1}$$

$$U_Q=Y\cdot m+(1-Y)\cdot m=m \tag{2}$$

$$\begin{aligned}\bar{U_A}&=X\cdot U_p+(1-X)U_Q\\&=X\cdot Y\cdot r+(Y-1)X\cdot g+m(1-X)\end{aligned} \tag{3}$$

根据平均收益可以看出：如果没有惩罚机制，即 g 为 0 时，从代理人的节点角度出发，若选择贿赂策略，收益会更大；当加入惩罚机制时，根据平均收益公式，g 越大时 X 也越大，则代理人节点的平均收益就越低，所以作为一个理性个体，若处罚力度越大（即举报节点的奖励收益越大），则代理人节点选择进行贿赂的概率就越小。同理，根据此收益分析表，从选民节点角度来看，只有竞选代理人节点对其进行贿赂才有可能获得额外收益，所以从理性选民节点角度来看，在遇到贿赂时选择举报或接受的概率与贿赂收益和奖励收益的多少有关。

3.3 收益函数的定义

本文定义了相应的收益函数来体现节点收到的奖励。

(1)投票收益函数

对于每一个参与投票的节点，系统会给予相应奖励，该奖励即为节点的收益。本文规定随着投票次数的增多，节点所得收益也会越多。投票收益的公式定义如下：

$$reward_{vote}=\begin{cases}\sum_{i=1}^{n}m(i+1)/8, & m\leqslant 2L/3\\ m/n, & m\geqslant 2L/3\end{cases} \tag{4}$$

其中，n 表示节点参与投票的总次数；i 表示投票的次数，从 1 开始递增；m 表示当前轮数参与投票的人数；L 表示总人数。

(2)基于时间成本的投票收益函数

基于时间成本的投票收益，是指节点只有在规定时间内完成代理人选举，系统才会发放奖励，而且完成时间越短，收益越大。基于时间成本的投票收益公式定义如下：

$$reward_T=\begin{cases}\sum_{i=1}^{n}(T-t)i, & t<T\\ 0, & t>T\end{cases} \tag{5}$$

其中，n 表示节点参与投票的总次数；i 表示投票的次数，从 1 开始递增；T 表示系统规定的时间；t 表示完成选举代理人工作所花的时间。

(3) 举报收益函数与贿赂收益函数

若节点发现贿赂节点并进行举报，系统将会对举报节点进行奖励，这就是举报收益。相应地，系统也会对贿赂节点进行处罚，节点接受贿赂所带来的好处就是贿赂收益。举报收益的公式定义如下：

$$Repotr=\beta\cdot m \tag{6}$$

其中，β 表示系统所设定的奖励力度；m 表示当前参与投票的人数。参与人数越多，则收益越高。

贿赂收益的公式定义如下：

$$Temp=\alpha\cdot i \tag{7}$$

其中，α 表示贿赂节点所给的贿赂力度，诱惑力度越大，则接受贿赂之后的非法收益也越多；i 表示节点接受贿赂的次数，节点接受贿赂的次数越多，则获得的非法收益也就会越大，下次选择接受贿赂的概率也会越高。

3.4 算法实现

算法 1 给出了基于投票奖励制度，节点 H 在第 i 轮参与投票时获得的收益。算法 1 第 2 步统计参与投票的人数并将其赋值给 m；第 3 步统计节点 H 的总投票次数；第 4 步统计参与投票节点和不参与投票节点的总数；第 5—8 步根据不同情况计算节点 H 投票所得的收益。

算法 1 节点参与投票时的奖励收益

```
Input:H,i // 输入要计算的节点以及投票轮数
Output:result[H] //节点 H 所得收益
1. Begin
2.   m=count(vote[i]) //统计在第 i 轮投票的节点数
3.   n=vote(node[H]) //统计节点 H 投票的次数
4.   L=count(vote[i]+not_vote[i])
5.     If (m≤2L/3)
6.       result[H]=∑(j=1 to n) m(j+1)/8
7.     Else
8.     result[H]=n/m
9. End
```

算法 2 给出了基于时间成本奖励制度，节点 H 在第 i 轮参与投票时获得的收益。算法 2 第 2 步确定参与投票的人数；第 3 步统计节点 H 的总投票次数；第 4 步统计参与投票节点和不参与投票节点的数量；第 5 步根据人数确定时间界限；第 6 步计算选举完成时间；第 7－8 步表示若在规定范围内完成则计算节点收益，否则节点投票收益为 0。

算法 2 在时间成本下节点参与投票的奖励收益

```
Input:H,i // 输入要计算的节点以及投票轮数
Output:result[H] //节点 H 所得收益
1. Begin
2.   m=count(vote[i]) //统计在第 i 轮投票的节点数
3.   n=vote(node[H]) //统计节点 H 投票的次数
4.   L=count(vote[i]+not_vote[i])
5.   T=calculate(m)
6.   t=election(H)
```

7. If t<T
8. result[H]=$\sum_{j=1}^{n}$(T−t)j
9. Else
   投票节点收益为 0
10. End

算法 3 表示在选举阶段，节点 H 在第 i 轮选举中选择举报还是接受贿赂。算法 3 第 3－4 步计算节点选择举报或是接受贿赂所得的收益；第 5－10 步统计节点在遇到贿赂节点时是接受还是举报，并增加相应举报概率及接受贿赂的概率，以方便下一轮的计算。

算法 3 节点在选举阶段选择举报还是接受贿赂

Input：H，i，k，j //输入节点、投票轮数、举报概率及接受贿赂概率
Output：result //选择举报还是接受贿赂
1. Begin
2. m=count(vote[i]) //统计在第 i 轮投票的节点数
3. Repotr=β×m //计算举报收益
4. Temp=α·i // 计算贿赂收益
5. if(report>Temp)
6. k=k+(β*10)% // 如果举报收益大于贿赂收益，则增加节点举报概率
7. else
8. j= j+(α*10)% //如果举报收益小于贿赂收益，则增加节点接受贿赂概率
9. result=Judge(k，j)//根据节点的举报概率及接受贿赂概率判断该节点采取的决策
10. End

4 实验仿真及分析

为了验证改进后的机制是否会吸引更多的节点进行投票以及是否能够有效减少贿赂节点，本文进行了仿真实验。在投票奖励实验中，仿真了 100 个独立节点，实现了 DPoS 共识机制中的原始投票模型，并将其与本文改进后的投票模型进行了对比。

4.1 机制改进前后参与投票节点的对比

以概率来表示节点参与投票的意愿，概率大于 0.5 表示该节点愿意参与投票，概率小于 0.5 则表示该节点不愿意参与投票。实验设置节点参加投票的初始概率为 0.5，经过 20 轮投票后，得到参与投票的节点数量变化图，如图 3 所示。

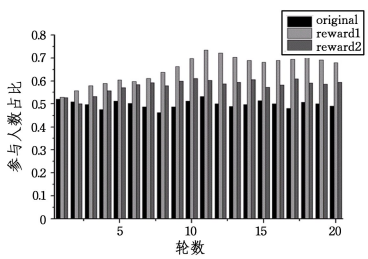

图 3 参与投票的节点数量变化图

Fig. 3 Variation diagram of number of voting notes

从图 3 可以看出，如果按照 DPoS 机制(original)进行投票，参与投票的总人数占 45%～50%。在投票就奖励(reward1)的改进方案下，由于收益函数设定收益的多少与参与投票的次数成正比，因此随着投票轮数的增多，参与投票的节点数越来越多，并最终保持在 65%～70%。因此，这个奖励制度适用于机制中节点积极性不高、总节点数量少并且容易受到恶意节点攻击的模型。在投票就奖励(reward1)的改进方案下可以吸引大多数节点参与其中，提高整体抵抗性。在基于时间成本奖励(reward2)的改进方案下，由于系统设定了超过时间限制则全员没有奖励的规则，因此参与投票的人数占比始终保持在 55%～60%之间(仍然多于没有改进之前参与投票的人数)。因此，这个奖励制在机制中能吸引一部分有能力的节点参与投票，并且激励节点在完成目标的前提下提高效率，节约了系统资源。

4.2 机制改进前后节点状态变化的对比

在模拟“贿赂、举报”这一仿真实验中，本文首先需要确定竞选代理人节点选择对选民进行贿赂(策略 P)的概率和不进行贿赂(策略 Q)的概率。我们假定在没有奖励与惩罚的机制下，恶意节点行贿被发现且接受处罚的概率为 20%，因此本文实验中规定初始选择 P(进行贿赂)策略的概率为 80%。在实验过程中，随着奖励力度(即处罚力度)的增大，选择 P 策略的概率会等比例下降。在选民节点 B 选择 E 策略(接受贿赂)还是 F 策略(选择举报)的概率设计上，我们采用 50%的初始概率，选民节点会根据收益分析表和收益函数计算公式进行每一轮的收益对比，如果举报收益高于贿赂收益，则选民节点选择这个策略的概率就会增加(力度越大则增加的概率也越大)，而且随着轮数概率可以叠加，反之亦然。

实验仿真每一轮都存在 20 个竞选代理人节点和 70 个选民节点，并规定每一个代理人节点会随机对 3 个选民节点做出贿赂或不贿赂的决策，选民节点再根据当前代理人节点的决策做出与之对应的决策。

本文实验仿真了选举阶段出现贿赂攻击的场景，首先对原始 DPoS 共识机制进行攻击，观察不同贿赂力度下节点状态的变化，然后对加入了“举报奖励”机制的选举阶段进行同样的贿赂攻击，观察不同贿赂力度下举报节点的数量变化。实验结果表明，“举报奖励”的共识机制可以很好地抵抗贿赂攻击。

原始 DPoS 机制下存在贿赂攻击的结果如图 4 所示。

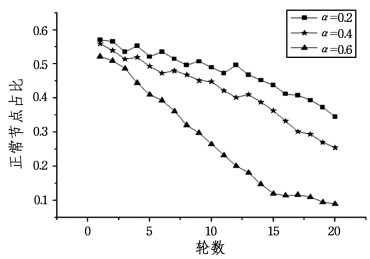

图 4 不同贿赂力度下 DPoS 机制中正常节点的占比

Fig. 4 Proportion of normal nodes in DPoS mechanism under different bribery intensities

由图 4 可以看出：正常节点(不接受贿赂的节点)占比随着投票轮数的增加而降低，而且随着贿赂力度 α 的增大，正常节点占比的下降速度越来越快，这也说明了 DPoS 共识机制对贿赂攻击抵御能力不够强壮的安全问题。

存在贿赂攻击时，改进 DPoS 机制的结果如图 5—图 7 所示。

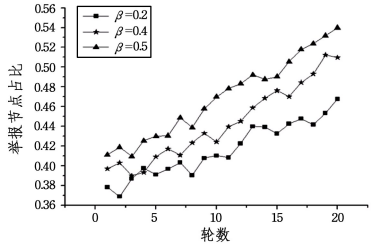

图 5 $\alpha=0.2$ 时不同奖励力度下举报节点的占比

Fig. 5 Proportion of reporting nodes under different incentives when $\alpha=0.2$

图 5 表示在贿赂力度 α 为 0.2 的情况下，系统采用不同的举报奖励力度时举报节点的总占比。可以看出，加入了举报奖励机制后，随着轮数的增加，举报节点也在不断增加。这就可以说明，面对贿赂攻击，加入了“举报奖励”机制后接受贿赂的节点随着轮数的增加越来越少，从而证明了改进机制可以有效抵御贿赂攻击。可以看出，在贿赂力度相同的情况下，随着奖励力度的增大，选择举报的节点增加的比例越来越高。

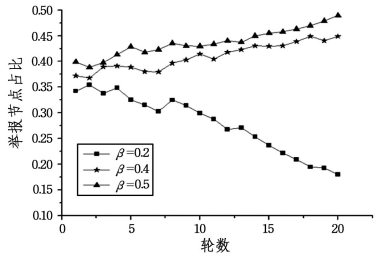

图 6 $\alpha=0.4$ 时不同奖励力度下举报节点的占比

Fig. 6 Proportion of reporting nodes under different incentives when $\alpha=0.4$

图 6 表示当贿赂力度 α 为 0.4 时举报节点的总占比。可以看出，奖励力度为 0.2 的情况下，举报节点的占比逐渐下降，这从另一个角度印证了理性选民节点采取了收益更大的方案(即接受贿赂)，这也符合现实推断。当奖励力度为 0.4 以及 0.5 时，可以看出，举报节点占比随轮数的增加而上升，意味着大多数节点采取了不接受贿赂的策略，这也证明了若存在中度贿赂攻击，改进后系统在提高奖励力度的情况下还能有效抵御贿赂攻击。

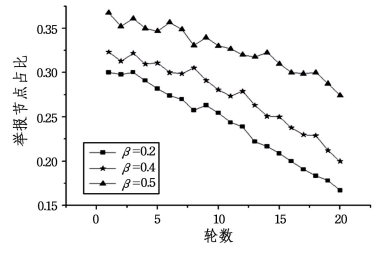

图 7 $\alpha=0.6$ 时不同奖励力度下举报节点的占比

Fig. 7 Proportion of reporting nodes under different incentives when $\alpha=0.6$

图 7 表示当贿赂力度 α 为 0.6 时举报节点的总占比。可以看出，在奖励力度小于贿赂力度的情况下，选择举报的节点数都在减少，但相比于同等贿赂力度情况下的未改进机制(随着投票轮数的增多，正常节点数几乎减少为 0)，加入了举报奖励机制的模型在投票后期还存在一些理性节点，而且当奖励力度为 0.4 和 0.5 时，举报节点仍然占一定比例，下降幅度不是很大。

以上实验证明了，本文提出的 DPoS 共识机制的改进极大地增强了系统的稳定性和节点抵抗贿赂的能力。

结束语 区块链是最近的研究热门，许多行业都在尝试使用区块链进行创新，文中对共识机制进行了研究与改进，解决了 DPoS 共识机制中存在的投票不积极以及选举过程中可能出现的腐败和贿赂选民问题，最后通过实验证明了加入奖励机制的可行性。本文提供了两种针对投票不积极现象对节点进行激励的方案，并讨论了这两种机制的优缺点以及适用的场景；其次，定义了“举报奖励”机制，其可以很好地防范恶意节点在选举中贿赂其他节点从而变成受托人的现象。然而，现实的 DPoS 机制在不同的应用场景下有不同的情况，系统中也会存在一些节点进行恶意投票来获取奖励的行为。未来，我们将主要关注恶意投票及恶意举报的问题，对这个机制做进一步的修改和完善；同时，也会进一步探讨采用怎么样的激励机制，才能达到一个最好的纳什均衡。

参 考 文 献

[1] WANG P, LIU X, CHEN J, et al. Poster: QoS-Aware Service Composition Using Blockchain-Based Smart Contracts[C]// 2018 IEEE/ACM 40th International Conference on Software Engineering: Companion Proceedings (ICSE-Companion). IEEE Computer Society, 2018.

[2] MERMER G B, ZEYDAN E, ARSLAN S S. An overview of blockchain technologies: Principles, opportunities and challenges [C]// Signal Processing & Communications Applications Conference. 2018.

[3] MENDLING J, WEBER I, AALST W V D, et al. Blockchains for Business Process Management-Challenges and Opportunities [J]. ACM Transactions on Management Information Systems, 2018, 9(1): 1-4.

[4] SINGH M, SINGH A, KIM S. Blockchain: A game changer for securing IoT data[C]// 2018 IEEE 4th World Forum on Internet of Things (WF-IoT). IEEE, 2018.

[5] YUAN Y, WANG F Y. Towards blockchain-based intelligent transportation systems[C]// 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC). IEEE, 2016.

[6] CHO H. ASIC-Resistance of Multi-Hash Proof-of-Work Mechanisms for Blockchain Consensus Protocols[J]. IEEE Access, 2018, PP(99): 1-1.

[7] ZHENG Z, XIE S, DAI H, et al. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends[C]// An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. IEEE Computer Society, 2017.

[8] HUANG J, KONG L, CHEN G, et al. Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism

[J]. IEEE Transactions on Industrial Informatics，2019，15(6)：3680-3689.

[9] XUE T，YUAN Y，AHMED Z，et al. Proof of Contribution：A Modification of Proof of Work to Increase Mining Efficiency [C]// IEEE Computer Software & Applications Conference. IEEE Computer Society，2018.

[10] GRAMOLI V. From blockchain consensus back to byzantine consensus[OL]. https://doi. org/10. 1016/j. future. 2017. 09. 023.

[11] NGUYEN C T，HOANG D T，NGUYEN D N，et al. Proof-of-stake consensus mechanisms for future blockchain networks：fundamentals，applications and opportunities[J]. IEEE Access，2019，7：85727-85745.

[12] SPASOVSKI J，EKLUND P. Proof of stake blockchain：performance and scalability for groupware communications[C]// Proceedings of the 9th International Conference on Management of Digital EcoSystems. ACM，2017：251-258.

[13] NGUYEN C T，HOANG D T，NGUYEN D N，et al. Proof-of-stake consensus mechanisms for future blockchain networks：Fundamentals，applications and opportunities[J]. IEEE Access，2019，7：85727-85745.

[14] LI W，ANDREINA S，BOHLI J M，et al. Securing proof-of-stake blockchain protocols[M]// Data Privacy Management，Cryptocurrencies and Blockchain Technology. Cham：Springer，2017：297-315.

[15] Peter G，Kiayias A，Russell A. Stake-bleeding attacks on proof-of-stake blockchains[C]// 2018 Crypto Valley Conference on Blockchain Technology (CVCBT). IEEE，2018.

[16] 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)：93-104.

[17] CHIU J，KOEPPL T. Incentive compatibility on the blockchain [R]. Bank of Canada，2018.

[18] LARS B，KIAYIAS A，KOUTSOUPIAS E，et al. Reward Sharing Schemes for Stake Pools[J]. arXiv：1807. 11218，2018.

[19] TANG C B，YANG Z，ZHENG Z L，et al. Game Dilemma Analysis and Optimization of PoW Consensus Algorithm [J]. Acta Automatica Sinica，2017，43(9)：1520-1531.

[20] 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 Development，2018，55(10)：2208-2218.

[21] MANSHAEI M H，JADLIWALA M，MAITI A，et al. A Game-Theoretic Analysis of Shard-Based Permissionless Blockchains [J]. IEEE Access，2018，PP(99)：1-1.

[22] WANG L X Y，QIN B，QIAO X. Development and Security of Blockchain Consensus Mechanism[J]. ZTE Technology Journal，2018，24(6)：12-16.

[23] FANG W D，ZHANG W X，PAN T，et al. Cyber Security in Blockchain：Threats and Countermeasures[J]. Journal of Cyber Security，2018，3(2)：87-104.

[24] KANG J，XIONG Z，NIYATO D，et al. Toward Secure Blockchain-Enabled Internet of Vehicles：Optimizing Consensus Management Using Reputation and Contract Theory [J]. IEEE Transactions on Vehicular Technology，2019，PP(99)：1-1.

[25] LUO Y，CHEN Y，CHEN Q，et al. A New Election Algorithm for DPos Consensus Mechanism in Blockchain[C]// 2018 7th International Conference on Digital Home (ICDH). IEEE，2019.

[26] WANG W，HOANG D T，XIONG Z，et al. A Survey on Consensus Mechanisms and Mining Management in Blockchain Networks[J]. arXiv：1805. 02707，2018.

[27] HAN X，YUAN Y，WANG F Y. Security Problems on Blockchain：The State of the Art and Future Trends[J]. Acta Automatica Sinica，2019(1)：206-225.

[28] SONG L H，LI T，WANG Y L. Applications of Game Theory in Blockchain [J]. Journal of Cryptologic Reseatch，2019，6(1)：100-111.

CHEN Meng-rong，born in 1994，postgraduate. Her main research interests indude combination of information security，block chain and consensus mechanism.

LIN Ying，born in 1973，Ph.D，associate professor. Her main interests indude information security.