文章编号:2096-7543(2022)03-0066-10 DOI:10.11863/j.suse.2022.03.09

基于信誉授权的DPoS共识机制改进研究

何 帅, 黄襄念

(西华大学计算机与软件工程学院,成都 610039)

摘 要:为了增强区块链公链系统中委托权益证明(DPoS)共识机制的"去中心化"程度以及提高节点投票的积极性,提出了一种改进方案。首先,利用基于算力竞争的PoW"挖矿"机制选出"代理节点"集合并设置节点的权益上限,然后通过投票机制从中选出"共识节点"集合,使得委托权益证明机制中共识节点的选举过程更加公平;同时,引入可验证随机函数对共识节点的出块顺序进行优化,增加了节点作恶的成本,防止恶意节点的"合谋攻击"。其次,利用博弈论中沙普利值的计算方式对出块节点获得的奖励进行合理分配,促进节点的投票积极性。最终,引入信用积分对节点的行为进行评判,结合节点当前所获得的投票权益和出块奖励计算综合信誉值(PCredit),并利用PCredit动态授权每轮参与共识的节点,增强其"去中心化"程度。实验结果表明,改进后的委托权益证明共识机制增强了系统的稳定性和安全性,在保证节点出块率的同时平衡了记账权竞争。

关键词:区块链;委托权益证明;可验证随机函数;博弈论;沙普利值

中图分类号:TP399 **文献标识码:**A

引 言

区块链技术是伴随着比特币的诞生而抽象出来的一种全新的分布式底层基础架构与计算范式,能够在缺乏第三方信任的机制下实现多方共识,不仅为数据隐私保护和安全传输提供了全新的技术支持,还提高了价值交互的效率[1]。区块链的本质是一种分布式共享数据库,是将数据按照时间顺序用类似链表的方式组成的数据结构[2],具有去中心化、数据防篡改、可追溯、不可伪造、多方共识的特性,已经在金融、航运物流、司法存证等领域得到了成功运用[3]。

目前,区块链已经形成了6层基础架构模型,由下往上分别为数据层、网络层、共识层、激励层、合约层以及应用层[4]。其中,共识层作为整个区块链架构的核心层,其共识算法保障了区块链网络数据的可验性和可信性,具有维护区块链系统稳定运行和节点相互信任的重要作用,是决定区块链系统中节点对账本数据的有效性和一致性达成共识的关键技术,其性能的优劣将直接影响整个区块链系统的去中心化程度、交易处理能力、安全性和可扩展性[5]。

当前区块链技术正面临着安全性、效率和去中心化的"不可能三角"问题,如何平衡三者之间的关系使得区块链更加安全高效成为了亟待突破的技术瓶颈[6]。针对现有区块链共识机制存在的不足之

收稿日期:2021-07-27
基金项目:国家自然科学基金资助项目(61902324)
作者简介:何 帅(1996-),男,硕士生,研究方向为区块链共识机制与跨链技术,(E-mail)2749267206@qq.com
通信作者:黄襄念(1964-),男,教授,博士,研究方向为模式识别,(E-mail)hslotus@stu.xhu.edu.cn

处，当前正围绕着共识节点的选举制度、恶意节点处理以及节点权益划分等[7]问题进行创新研究，力争研发出适用于更多区块链场景的高效共识算法。

目前，在区块链公链系统中主流的共识机制有工作量证明（PoW）、权益证明（PoS）以及委托权益证明（DPoS）[8]。PoW是基于自身算力竞争来求解一个难以计算但容易验证的Hash数学难题，使得率先解决Hash难题并得到其他节点有效验证后的节点拥有记账权并获得奖励[9]。但PoW在达成共识过程中会消耗大量的算力造成资源浪费，并且打包交易数据产生新区块的时间通常在10 min以上，这显然无法满足复杂的业务需求。为了解决PoW共识算法中存在的资源浪费以及“挖矿”不公平等问题，有学者提出了PoS共识机制，通过利用PoS取代基于算力的工作量证明来决定节点获得记账的权力，但当财富积累到一定的程度时，容易出现集权现象，导致币龄大的节点始终掌握着记账的权利，从而出现“财阀统治”的局面，不仅增加了中心化的风险，还降低了虚拟货币的流通性[10-11]。为了进一步满足广泛的区块链业务需求，Larimer在PoS的基础上通过优化选择记账节点的过程，提出了DPoS共识机制[12]，实现了快速共识验证，提高了区块链系统达成共识的效率，进一步减少了资源的浪费并弱化了通过矿池算力叠加造成的中心化风险，增强了区块链系统的安全性。但DPoS在实际的应用过程中还存在节点投票不积极、恶意节点贿赂投票节点导致“腐败攻击”以及权益分配不合理等相关问题，这正是当前亟待突破的关键方向。

为了提高区块链的安全性和共识效率，针对上述委托权益证明共识机制存在的不足之处，相关研究学者对其展开了新一轮的探索与创新。付瑶瑶等[13]针对DPoS共识机制中节点投票不积极以及恶意节点作恶问题，提出了一种基于奖励机制和信用机制改进的方案，利用一种改进的收益分配算法合理分配各节点所得的权益，并通过优化投票结果的计算方式加大恶意节点成为代理节点的难度，在一定程度上降低了恶意节点成为共识节点的概率，提高了系统的安全性。杨坤桥等[14]对DPoS共识机制的计票机制和激励机制进行了改进，使得改进的计票机制能够更加全面的反映节点的信用情况，并根据节点选票权重快速剔除恶意节点，同时改进的激励机制能够对节点收益进行二次分配，提高了系统“去中心化”程度。在上述相关研究成果的基础之上，本文利用基于算力竞争的PoW“挖矿”思想，结合可随机验证函数，引入博弈论中沙普利值的计算方式对DPoS共识算法的投票选举、见证人出块顺序以及节点的权益分配进行了改进和优化，最后通过仿真实验得出结论。

1　委托权益证明共识机制的改进方案

委托权益证明（DPoS）共识算法主要包含两个步骤，即共识节点的选举过程以及节点间达成共识的过程[15]。针对DPoS共识算法中存在的不足之处，对共识节点选举、共识节点的出块顺序、奖励的分配以及节点出块行为监测进行改进和优化，整体改进流程如图1所示。

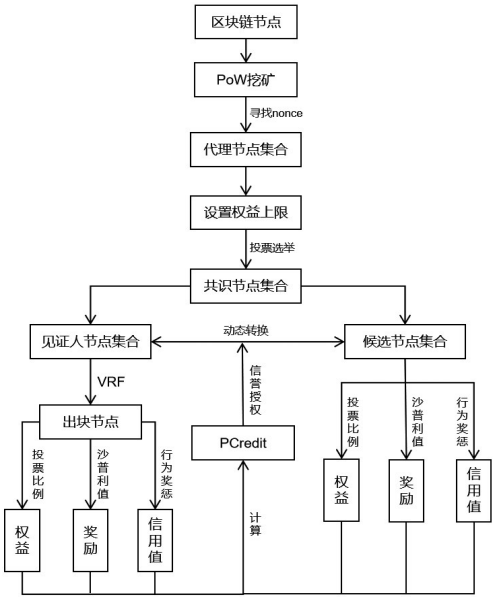


图1　委托权益证明共识机制的改进流程

区块链节点首先通过PoW“挖矿”机制筛选出部分节点组成代理节点集合，同时为代理节点集合中的节点设置权益上限，并通过投票机制选出共识节点集合。在共识节点集合中，获得投票权益更高的节点组成见证人节点集合参与区块的打包和验证；剩余的节点成为候选节点集合，用于及时替换见证人节点集合中出现异常行为的节点。在出块过程中，通过可验证随机函数（VRF）随机选择见证

人节点集合中的节点参与区块打包,并通过信誉积分对节点行为进行评断,同时利用沙普利值的计算方式对成功出块的节点所获得的系统奖励进行合理分配。最后,将出块节点当前的信用积分、所获得的投票权益以及系统奖励作为指标计算其综合信誉值(PCredit),并利用PCredit值动态调整见证人集合和候选节点集合中的节点,尽最大可能保证每一轮共识过程中所有见证人节点都能正常打包区块,提高系统的稳定性和安全性。

1.1 改进的共识节点选举机制

针对DPoS共识机制中共识节点选举公平性问题,对其做出如下优化:

(1)利用PoW机制完全去中心化的特性对DPoS共识机制的节点选举过程进行改进。首先,设置节点挖矿的时间来动态调整PoW机制中哈希计算的难度值,使得区块链系统中大多数节点都能公平地参与记账权的竞争,并规定在设置的时间内能够找到随机数nonce的节点将成为代理节点,为共识节点的进一步选举做了初步筛选[16]。通过降低并动态调整哈希计算的难度值,能够让更多的算力较小的节点也能有机会成为共识节点,体现出选举的公平性。

在PoW共识机制中,当难度值为n时,节点基于自身算力通过蛮力法不断地进行哈希碰撞以求解满足要求的随机数nonce,使得求解出的nonce值拼接前一区块的哈希值(PreHash)再次进行哈希计算得出的哈希值(CurHash)满足前n位为0,即挖矿成功[17]。当前,PoW始终保持每10 min左右打包一个区块,其难度值的计算公式如式(1)所示:

$$curD = preD \times (20160/allTime) \tag{1}$$

在上式基础上对PoW的难度值的计算方式进行调整,设置允许节点参与挖矿的时间为60 s。为了满足更多节点基于算力挖矿的条件,将挖难度值设置为5,此时大部分节点能够在几十秒内挖矿成功,找到满足要求的随机数nonce。同时,为了提高选举效率,当成功创建360个区块时进行一次难度调整,由于挖矿时间设置为60 s,因此相当于每6 h调整一次难度值,改进后的难度值计算公式如式(2)所示:

$$curD = preD \times (21600/totalTime) \tag{2}$$

式(1)~(2)中:*curD*表示当前区块的难度值,*preD*表示前一区块的难度值,*allTime*表示创建2016个区块所花的总时间,其值接近于20160,单位为min;*totalTime*表示创建360个区块所花的总时间,其值接近于21600,单位为s。

通过对PoW挖矿时间的限制和难度值的调整,使得能够在60 s内挖矿成功的节点进入代理节点集合,为共识节点的选取做了初步筛选[18]。在节点计算哈希难题时,如果当前节点的算力较大时,其挖矿时间可能少于60 s,则21600/*totalTime*将大于1,此时*curD*将大于*preD*;如果当前节点的算力较小时,其挖矿时间可能大于60 s,则21600/*totalTime*将小于1,此时*curD*将小于*preD*。故通过对挖矿难度的动态调整能够让更多算力不同的节点公平地竞争出块权。

(2)为了防止持币量大的节点恶意攻击,对利用PoW筛选出来的节点和投票节点设置权益上限。由于DPoS是在PoS机制上演进而来的具有更高效率的共识机制,因此在投票过程中继承了PoS中币龄的概念,通过权益投票选择共识节点[19]。在DPoS中节点的权益用币龄表示,即币龄等于所持代币数与持币时间的乘积[21],如式(3)所示:

$$coinAge = coinCount \times coinTime \tag{3}$$

其中:*coinAge*表示节点的币龄,*coinCount*代表节点所拥有的代币数,*coinTime*表示持币时间。

在式(3)的基础上,对节点的币龄设置上限,规定币龄最大值(*mCoinAge*)为2000,同时规定所有节点持币时间的最大值(*mCoinTime*)为30 d,则币龄计算如式(4)所示:

$$mCoinAge = coinCount \times mCoinTime \tag{4}$$

从上式可以看出,当节点持币时间达到最大值或者币龄本身达到自身设置的最大值时,节点的币龄均不会再增长,不仅能够限制见证人节点可接受的最大投票总量,避免“财阀统治”[20]局面的出现,还能促使持有大量token的节点将权益投给多个见证人节点以获得更多的投票回报奖励,从而平衡节点的出块概率,降低“贿赂攻击”[21]的几率。

(3)权益持有者通过投票机制将自身持有的token委托给代理节点集合中的节点,并在节点最大权益限制的情况下根据代理节点中节点获得的权

益投票比例进行排序，选出排名前30的节点组成共识节点集合，其中排名前21的节点组成见证人节点集合，剩余节点组成候选节点集合。假设代理节点集合中节点i有n个权益投票人，则其最终获得的投票权益计算如式(5)所示：

$$V_i^{\text{total}} = \min\left(mCoinAge, \sum_{j=1}^{n} Node_j^{coinAge} \times \frac{mCoinAge - V_i^{coinAge}}{mCoinAge}\right) \tag{5}$$

其中：V_i^{total}表示代理节点集合中第i个节点最终获得的投票权益，$mCoinAge$表示节点权益上限，$Node_j^{coinAge}$表示第j个投票节点拥有的权益值，$V_i^{coinAge}$表示代理节点集合中第i个节点当前权益值。

1.2　优化共识节点出块机制

在区块链系统中，DPoS共识算法所维护的见证人节点集合中所有节点均获得记账权后称为完成一轮共识，当某一个见证人节点获得记账权并完成区块的打包后称为完成一次共识过程。在传统的DPoS共识协议中，每一轮共识过程都是按照既定的见证人节点顺序参与区块的打包，恶意节点能够通过已知的出块顺序发起合谋攻击[21]。为了减少被攻击的概率，对见证人节点的出块顺序进行改进，利用可验证随机函数(VRF)[22]改变每轮参与共识的节点顺序，增加恶意节点攻击的成本，防止合谋攻击。

利用VRF生成随机数来确定见证人节点的出块顺序，其随机数的生成及验证过程如下：

(1)生成一对公私钥，分别为$pubKey$和$priKey$。

(2)生成随机数：

$RanNum = VRF\_HASH(priKey, hashValue)$。

(3)生成验证数：

$VerNum = VRF\_PROOF(priKey, hashValue)$。

(4)将$RanNum$和$VerNum$广播给验证者进行如下计算：

$RanNum = VRF\_P2H(VerNum)$。

(5)当第4步验证通过，则对当前区块哈希值进行验证：

$VRF\_VERIFY(pubKey, hashValue, verNum)$。

(6)如果第5步中函数的返回值是TRUE，则验证通过；若函数返回值为FALSE，则表明产生的随机数被篡改。

利用VRF生成的随机数在见证人节点集合中选取出块节点，计算如式(6)所示：

$$RanNode = RanNum\%NodeNum \tag{6}$$

其中：$RanNode$表示本次获得出块权力的见证人节点编号，$RanNum$表示利用可验证随机函数生成的随机数，$NodeNum$表示见证人节点集合中节点数量。

在出块节点选取过程中，将当前负责出块的见证人节点的私钥设置成$priKey$，并通过当前区块的哈希值$hashValue$生成$RanNum$和$VerNum$。当利用VRF生成随机数选取下一个出块节点时，前一个出块节点会将计算出的$RanNum$和$VerNum$广播给其他见证人节点，此时其它的见证人节点可以对随机数和下一个出块节点进行验证，如果超过2/3的节点通过验证，则说明随机数未被篡改，下一个出块节点将被确定。算法1概括了优化后的见证人节点出块机制。

算法1： witnessNodeBlockProcess()

输入：密钥对($pubKey$,$priKey$)和当前区块哈希值$hashValue$。

输出：见证人节点集合中出块节点的序号$RanNode$。

```
Begin
RanNum = VRF_HASH(priKey,hashValue)//生成随机数
VerNum = VRF_PROOF(priKey,hashValue)//生成验证数
RanNum = VRF_P2H(VerNum)//对随机数进行验证
VRF_VERIFY(priKey,hashValue,VerNum)// 验证区块hashValue
RanNode = RanNummodNodeNum//确定出块的节点
Return RanNode
End
```

1.3　改进的奖励分配机制

针对DPoS算法中权益分配不均以及节点投票不积极问题，利用博弈论中沙普利值的计算方式对见证人节点的区块奖励进行合理分配。

在博弈论中，根据局中人之间是否存在约束力将博弈分为合作博弈与非合作博弈[23]。在DPoS共识机制中，当不同的权益持有者给同一个目标节点投票时，此目标节点与投票的节点将形成了一个“利益共同体”，只有当目标节点成为见证人节点

后,投票节点才能获得最大收益。因此,给同一见证人节点投票的节点之间形成了合作博弈的关系[24]。在合作博弈中,主要讨论的对象是联盟以及如何解决联盟中每个局中人的收益分配问题。

本文将DPoS共识机制中给同一个目标节点投票的所有节点形成的"利益共同体"[25]集群称为一个联盟N,联盟中的节点称为局中人,为每一个联盟定义一个价值函数V,并规定$V(\phi)=0$,则联盟博弈可以表示为(N,V)。在DPoS的投票博弈中,每个局中人在联盟中的边际贡献称为沙普利值,若某个联盟获得总投票权益的一半,则该联盟获胜,目标节点将成为见证人节点;同时,为了限制节点投票的时间,防止节点无限期拖延投票,将时间作为节点沙普利值计算的一个因素。若用W表示获胜的联盟,则对于任意的子联盟S其价值函数定义如式(7)[24]所示:

$$V(S)=\begin{cases}1, & S\notin W\\ 0, & S\in W\end{cases} \tag{7}$$

则此时联盟S中节点i的沙普利值如式(8)[25]所示:

$$\phi_i(N,V)=\frac{1}{|N|!}\sum_{S\subseteq N\setminus\{i\}}|S|!\left(|N|-|S|-1\right)!\times\left[V\left(S\cup\{i\}\right)-V(S)\right] \tag{8}$$

其中$\phi_i(N,V)$为联盟S中局中人i的平均边际贡献。当局中人i不在联盟S中时,其中每个局中人的沙普利值取之前的局中人形成联盟的边际递增价值,则当第i个局中人加入联盟S后其边际贡献为$V\left(S\cup\{i\}-V(S)\right)$。此时,在节点$i$之前的局中人有$|S|!$种排列方式,在节点$i$之后的局中人有$(|N|-|S|-1)!$种排列方式[25]。因此,联盟$S$共有$|S|!\times(|N|-|S|-1)!$种边际贡献,然后求和并取均值。

加入时间因素后的节点沙普利值式(9)所示:

$$\phi_i^T(N,V)=\frac{\phi_i(N,V)}{T_i-T_{\text{vote}}} \tag{9}$$

其中:T_i表示节点i投票结束的时间,T_{vote}表示发起投票的时间。当T_i-T_{vote}越小则说明节点投票花费的时间越少,此时分母越小节点的沙普利值越大,从而能够促进更多的节点在规定时间范围内参与投票。

假设见证人节点i有n个投票节点,当成功出块后获得的出块奖励为RB_i,则每个投票节点的奖励如式(10)所示。通过沙普利值为该见证人节点投票的节点分配奖励后,该见证人节点最终获得的区块奖励为R_i,如式(11)所示。

$$voteNodeR_j=RB_i\times\phi_j^T(N,V) \tag{10}$$

$$R_i=RB_i\left(1-\sum_{j=1}^{n}\phi_j^T(N,V)\right) \tag{11}$$

区块链系统的激励机制是保证系统按照既定的规则稳定运行的关键[26]。因此,更加合理的节点奖励分配制度能够避免节点通过作恶的方式获取更多的收益,提高节点参与共识以及投票的积极性。通过引入了博弈论中沙普利值的计算方式对见证人节点打包区块所获得的系统奖励进行合理分配,以奖励回报的方式鼓励更多的节点保持在线并积极参与投票,使得更多的小节点通过投票获得一定的收益,提高其成为共识节点的机会,从而增强去中心化程度,不仅能够解决区块链系统中节点的"社会分层"现象[27],还能够使得见证人节点和投票节点之间形成利益共同体,共同维护系统的安全和稳定。算法2概括了改进后的节点奖励分配机制。

算法2: blockRewardDistribution()

输入:联盟S中的节点集合N、第j个见证人节点的出块奖励RB_j,投票节点个数n。

输出:联盟S中每个节点获得的奖励。

Begin

$j\leftarrow 1$,Initial(V)//初始化价值函数

while$(j\leqslant n\&\&N_j\in S)$

$\phi_j(N,V)=\frac{1}{|N|!}\sum_{S\subseteq N\setminus\{i\}}|S|!\left(|N|-|S|-1\right)!\times\left[V\left(S\cup\{i\}\right)-V(S)\right]$

$T=T_j-T_{vote}$//节点j投票花费的时间

$\phi_j^T=\frac{\phi_j(N,V)}{T}$//计算节点$j$的边际贡献

$voteNodeR_j=RB_j\times\phi_j^T(N,V)$//计算投票节点的奖励分配

$j++$

Return $voteNodeR_j$

End

1.4 见证人节点动态转换机制

DPoS共识机制中对异常节点并没有及时的处理方式,而是在下一轮投票中将恶意节点通过投票的方式投票出局[28]。但为了保证算法的高效性,

DPoS共识机制的见证人集合会维持一定的时间段后再进行下一轮投票，通常都是利用锁定机制进行投票，例如在企业运营系统（EOS）项目中，见证人节点集合锁定每24 h进行一次投票更新，从而防止因为频繁投票而降低系统的性能[29]。因此，在下一轮投票开始之前，该异常节点还有机会参与出块。如果该节点是因为节点宕机、断电、网络延迟等不可避免的因素出现异常行为，则在后面可能恢复正常。但如果该节点本身就是恶意节点，那么在下一轮共识过程中该节点可能持续作恶，导致出块延迟、交易堵塞等问题。因此，本文在将通过投票系统选出的共识节点集合分为了见证人节点集合和候选节点集合，当见证人集合中某个节点出现异常行为时，将通过动态转换机制将异常节点和候选节点集合中的节点及时进行替换，以保证在下一轮共识中所有节点均能正常打包区块。

在见证人节点动态转换机制中，每一轮投票结束后给共识节点集合中的所有节点初始化一个信誉值（*Credit*），通过信誉积分对见证人节点的行为进行评断，且初始赋值为100。当每次见证人节点出现异常行为时扣除10，每次正常出块后信誉值增加1，通过节点信誉值丢失容易而难以积累的机制来限制节点作恶的行为；同时结合该节点所获得的投票权益以及当前所获得的系统奖励计算节点的综合信誉值（*PCredit*），并通过*PCredit*对节点进行动态转换。其中第i个见证人节点的*PCredit*如式（12）所示：

$$PCredit_i = \alpha \times V_i^{\text{total}} + \beta \times R_i + \gamma \times Credit_i \quad (12)$$

其中：$\alpha + \beta + \gamma = 1$，并设定权益的权重为$\alpha = 0.2$，区块奖励的权重为$\beta = 0.3$，信誉积分的权重为$\gamma = 0.5$。由于每一轮投票后，共识节点集合中的节点会进行一次更新，而投票权益也会随之更新，重新选出投票权益较大的节点构成共识节点集合，因此权益的权重系数最小；而信誉值只是给每一轮投票后产生的节点进行初始化赋值，其他普通投票节点并没有信誉值，因此为了体现公平性，每次投票前均需要将上一轮投票选出的共识节点中所有节点的信誉值归零处理，在下一轮投票选出共识节点集合后重新进行信誉值初始化，使得信誉值只对当前这一组共识节点进行行为评断，并通过信誉奖惩及时处理恶意节点，因此信誉权重最大；同时，节点通过沙普利值分配得到的奖励是节点通过长期积极投票或者有效出块所积累的，因此在计算*PCredit*中系统奖励所占权重比权益所占权重大，使得即使是算力大的节点也不能仅仅通过当前的算力优势获得记账权。

在进行第一轮共识时，共识节点集合中所有节点的信誉值均相等，而见证人集合中的节点的投票权益比候选节点集合中节点的投票权益多，初始的系统奖励均为0。当见证人节点集合中的节点完成一轮共识后，系统将计算见证人节点集合中所有节点的*PCredit*，当节点的*PCredit*低于系统设定的阈值时将自动退出见证人节点集合，此时候选节点集合中*PCredit*最大的节点将自动依次进入见证人节点集合去填补见证人节点集合中退出的节点；当完成一轮共识后，见证人节点集合中节点的*PCredit*均大于系统设定的阈值时，此时见证人集合中的节点将依次与候选节点集合中的节点的*PCredit*进行比较，用候选节点集合中*PCredit*更大的节点去替换见证人节点集合中*PCredit*相对较小的节点。通过*PCredit*值对见证人节点进行动态转换能够及时对异常节点进行处理，提高系统运行的稳定和安全性，见证人节点动态转换机制如图2所示。

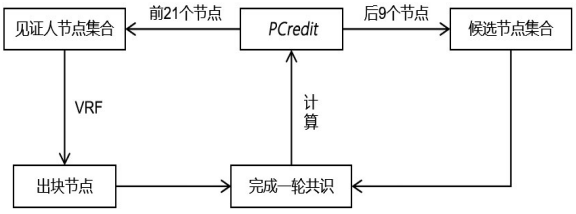


图2　见证人节点动态转换流程

2　实验结果及分析

2.1　实验环境

为验证改进后的DPoS算法的有效性，在相同的模拟环境下从多个维度对DPoS算法改进前后进行验证分析。实验在处理器Intel® CoreTM i7-7700 CPU@ 3.6 GHz的64位Windows 10企业版平台上，在go1.16windows-amd64环境下利用Go语言模拟了DPoS算法，采用Geth搭建101个以太坊节点集群。

最后,通过MATLAB R2016b对最终的实验数据进行可视化对比评价。

2.2 算法验证

2.2.1 节点安全性验证

在DPoS共识机制中,共识节点选取过程的公平性和安全性将直接影响整个区块链系统的性能。为了验证改进后的DPoS共识算法在节点选取阶段是否能提高共识节点的可信度,在恶意节点占比30%的情况下通过多轮投票并统计对比了每轮选出的共识节点集合中诚实节点所占的比例,实验结果如图3所示。从图3中可以看出,改进后的DPoS共识算法通过投票机制选出的共识节点集合中诚实节点所占比例更高;且随着投票轮次的增加,共识节点集合中诚实节点的占比逐渐增加并保持在92%左右,而传统的DPoS共识算法选出的共识节点集合中诚实节点所占比例最终保持在83%左右。实验结果表明,利用PoW挖矿机制对节点进行初步筛选,能够让更多节点基于算力通过更加公平的竞争成为共识节点;同时,在此基础上通过对节点权益设置上限有效地避免了权益大的节点之间的"贿赂攻击",从而降低了恶意节点成为共识节点的几率。

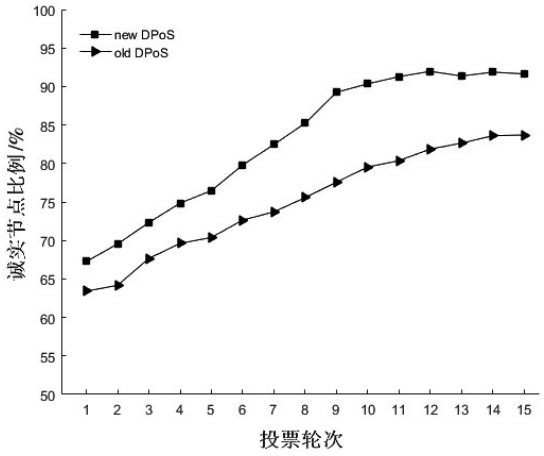


图3 共识节点集合中诚实节点比例

此外,为了验证改进后的DPoS共识机制的容错性,在共识过程中通过断网的方式模拟见证人节点遭受攻击成为恶意节点的情况。当存在3个恶意节点时,统计了在50轮共识过程中共识节点产生有效区块的个数,其结果如图4所示。从图4中可以看出,在相同的模拟环境下,改进后的DPoS共识机制能够产生更多的有效区块,这是因为改进后的DPoS共识机制中能够通过见证人节点动态转换机制及时处理恶意节点,当节点出现恶意行为时,系统能够利用信用惩罚的方式通过备用节点集合对恶意节点进行及时替换,不需要通过下一轮投票剔除恶意节点,使得即使存在恶意节点的情况下也能保证在下一轮共识过程中尽最大可能产生有效区块,提高了系统的容错性,在一定程度上提高了系统的吞吐率和安全性。

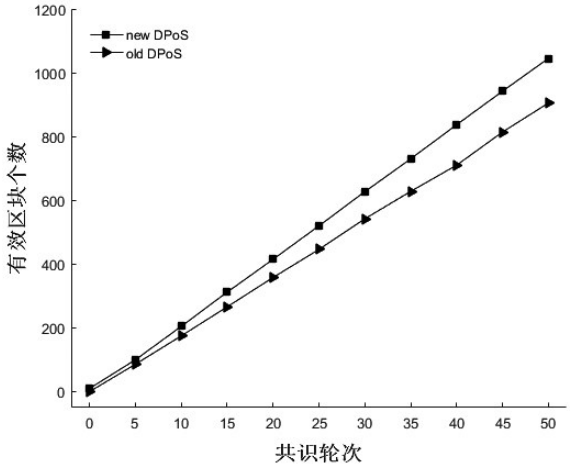


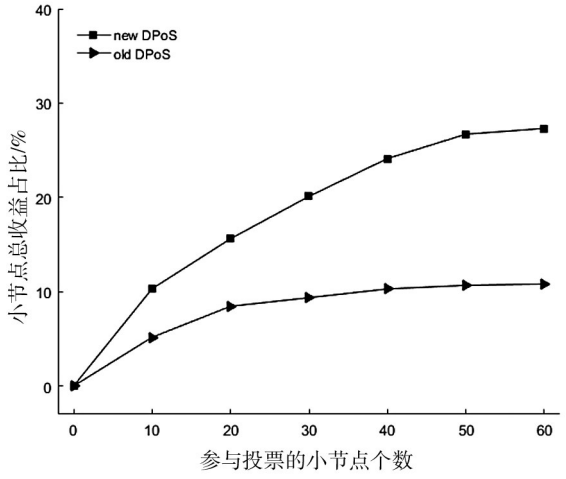
图4 共识机制容错率对比

2.2.2 节点奖励分配与投票积极性验证

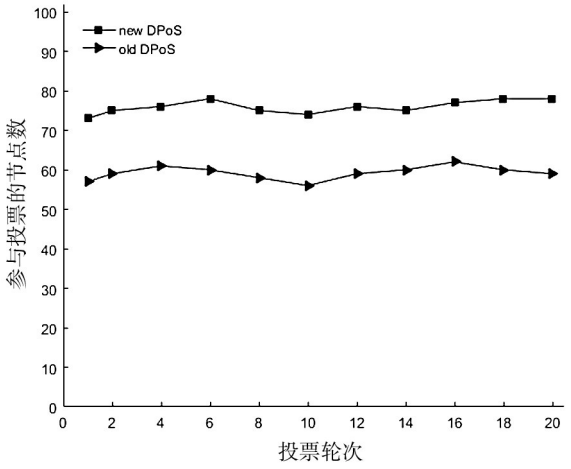
在DPoS共识机制中,由于只有部分代表节点参与区块的打包和验证,使得区块链系统中大部分节点长期处于不在线的状态。本文为了验证博弈论中沙普利值的计算方式对区块奖励均衡划分以及对促进节点积极投票的有效性,在相同的环境下对改进前后的DPoS共识机制进行了20轮共识过程,对两种算法中投票节点获得的区块奖励以及参与投票的节点数量进行了统计和对比,其结果如图5所示。

在共识节点的选举过程中,参与投票的节点大多数都是小节点。在本文的改进过程中,由于对节点的权益设置了上限,使得拥有较大权益的节点也不能将自身持有的权益投给一个节点,而是将自身权益分投给多个节点。因此,小节点的奖励分配将直接影响其投票的积极性。从图5(a)中可以得出,改进后的DPoS共识机制中,随着投票节点中小节点个数的增加,小节点总体获得的奖励比重持续增加,而传统DPoS共识机制中,小节点获得的奖励并没有明显提高。这是因为在传统的DPoS共识机制

中,投票节点最终获得的奖励是根据自身投票权益所占的比重进行分红,使得那些大节点始终占据主导地位,从而加剧节点之间的“贫富差距”;而利用沙普利值通过每个投票节点的边际贡献对区块奖励进行分配,有利于使小节点获得的收益更加合理。同时,在拥有101个区块链节点的集群中进行20轮的共识投票,对积极参与投票的节点进行统计分析,其结果如图5(b)所示,改进后的DPoS共识机制能促进更多的节点参与共识投票,表明利用沙普利值对区块奖励进行分配不仅能够避免大节点的“财阀统治”,还能促进更多的节点保持在线,共同维护系统安全。



(a) 基于沙普利值的奖励分配



(b) 参与投票的节点统计

图5　节点奖励分配与投票积极性

2.2.3　时间效率对比分析

对比分析了20轮共识过程中DPoS共识机制改进前后的时间消耗,结果如图6所示。

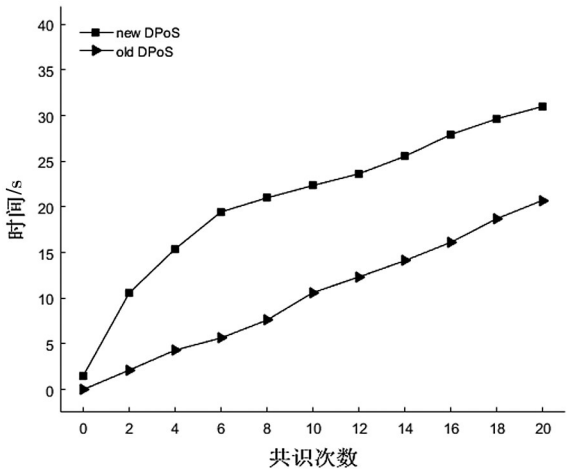


图6　时间效率对比

从图6中可以看出,改进后的DPoS共识算法略大于传统的DPoS共识算法的时间消耗。因为在DPoS共识机制的整体改进过程中,为了让大部分节点拥有更公平的机会参与到记账权竞争中,在共识节点选举的前期阶段利用了工作量证明中的挖矿机制对节点进行了初步筛选,但挖矿机制是基于数学难题的哈希计算,相对于传统DPoS中的直接委托投票选举而言,其时间消耗必然增加。因此为了平衡节点共识的公平性和整体时间开销,限制了挖矿的难度并锁定了节点挖矿时间为60 s左右。在共识阶段,传统DPoS共识机制是按照既定的顺序依次打包区块;为了防止恶意节点的有效攻击,本文利用可验证随机函数(VRF)增强了打包区块的共识节点的随机性,强化了共识过程的安全性,但VRF的引入在一定程度上也增加了系统的开销。在权益分配阶段,传统DPoS共识机制中各节点的最终权益是根据委托比重进行分红;为了让更多小节点获得更多的权益,本文基于节点对共识过程中的贡献利用沙普利值对权益进行了合理划分,促进了更多节点积极参与到共识过程中来共同维护系统的稳定,但同时也增加了整体算法的复杂度,因此改进后的DPoS算法需要花费更多的时间。

综上分析,虽然改进前后两种机制的时间消耗有所不同,但并没拉开太大的差距,总体上提高了系统的安全性,且DPoS共识机制目前主要运行在

EOS系统中,能够容忍秒级单位范围内的时间消耗。因此,综合考虑区块链系统的稳定性和效率,改进后的DPoS算法能够在相对高效的时间效率下更好地保证出块的安全。

3 结束语

为了兼顾区块链公链系统效率与其安全性,本文从共识节点的选举、见证人节点出块顺序以及权益分配方面进行了改进和优化。通过PoW算法的“挖矿”机制增强了共识节点选举的公平性,提高了小节点成为共识节点的几率;同时,利用可验证随机函数优化了见证人节点打包区块的顺序,增加了节点作恶的成本,在一定程度上防止了“合谋攻击”的现象;最后,利用沙普利值的计算方式实现了对节点奖励分配的均衡化,有效地避免了区块链系统中“财阀统治”的局面,促进了节点投票积极性。实验结果表明,本文的改进方法对DPoS共识协议的安全性有所巩固,在保证算法高效出块的情况下平衡了记账权的竞争。但仍存在一些不足之处,在增强共识节点选举公平性的同时,如何进一步减少时间开销以及如何使得节点的权益分配达到纳什均衡将是接下来的重要研究工作。

参考文献:

[1] 唐长兵,杨珍,郑忠龙,等.PoW共识算法中的博弈困境分析与优化[J].自动化学报,2017,43(9):1520-1531.

[2] 郑敏,王虹,刘洪,等.区块链共识算法研究综述[J].信息网络安全,2019(7):8-24.

[3] 王缵,田有亮,李秋贤,等.基于信用模型的工作量证明算法[J].通信学报,2018,39(8):185-198.

[4] 刘艺华,陈康.区块链共识机制新进展[J].计算机应用研究,2020,37(S2):6-11.

[5] 吴梦宇,朱国胜,吴善超.基于工作量证明和权益证明改进的区块链共识机制[J].计算机应用,2020,40(8):274-278.

[6] 靳世雄,张潇丹,葛敬国,等.区块链共识算法研究综述[J].信息安全学报,2021,6(2):85-100.

[7] 董振恒,吕学强,任维平,等.高性能区块链关键技术研究综述[J].数据分析与知识发现,2021,5(6):14-24.

[8] 谈森鹏,杨超.区块链DPoS共识机制的研究与改进[J].现代计算机(专业版),2019(6):11-14.

[9] 陈梦蓉,林英,兰微,等.基于“奖励制度”的DPoS共识机制改进[J].计算机科学,2020,47(2):269-275.

[10] 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.

[11] 田炽招.公有区块链共识算法研究与改进[D].深圳:深圳大学,2018.

[12] 闵新平,李庆忠,孔兰菊,等.许可链多中心动态共识机制[J].计算机学报,2018,41(5):1005-1020.

[13] 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.

[14] 杨坤桥,王煜翔,郭兵,等.委托股权证明共识机制的改进研究[J].计算机工程与应用,2021,57(24):107-114.

[15] 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.

[16] 廖浩德,邹晓凤,王兵,等.模糊随机碰撞工作量证明共识算法[J].计算机工程与应用,2022,58(7):137-141.

[17] 夏清,窦文生,郭凯文,等.区块链共识协议综述[J].软件学报,2021,32(2):277-299.

[18] 何泾沙,张琨,薛瑞昕,等.基于贡献值和难度值的高可靠性区块链共识机制[J].计算机学报,2021,44(1):162-176.

[19] 钟增胜.一种基于区块链PoS共识算法的改进研究[J].重庆工商大学学报(自然科学版),2021,38(4):36-41.

[20] 甘俊,李强,陈子豪,等.区块链实用拜占庭容错共识算法的改进[J].计算机应用,2019,39(7):2148-2155.

[21] HUANG J H,XIA X,LI Z C,et al.Trust proof mechanism based on dynamic authorization[J].Journal of Software,2019,30(9):2593-2607.

[22] 李希之.基于可验证随机函数的拜占庭容错共识算法的改进与实现[D].南京:东南大学,2019.

[23] WANG Y H,CAI S B,LIN C L,et al.Study of blockchains's consensus mechanism based on credit[J].IEEE Access,2019,7:10224-10231.

[24] 高迎,谭学程.DPOS共识机制的改进方案[J].计算机应用研究,2020,37(10):3086-3090.

[25] 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.

[26] 林晖,于孟洋,田有亮,等.移动云计算中基于动态博弈和可靠推荐的传递信誉机制[J].通信学报,2018,39(5):85-93.

[27] 隋凯凌.CyberMiles中DPoS共识机制的分析与改进[D].大连:大连海事大学,2019.

[28] 毛梦晴.DPoS共识算法选举机制的分析与优化[D].重庆:重庆邮电大学,2020.

[29] 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.

引用格式:

中　文:何帅,黄襄念.基于信誉授权的DPoS共识机制改进研究[J].四川轻化工大学学报(自然科学版),2022,35(3):66-75.

英　文:HE S,HUANG X N.Research on improvement of DPoS consensus mechanism based on reputation authorization[J].Journal of Sichuan University of Science & Engineering(Natural Science Edition),2022,35(3):66-75.

Research on Improvement of DPoS Consensus Mechanism Based on Reputation Authorization

HE Shuai, HUANG Xiangnian

(School of Computer & Software Engineering, Xihua University, Chengdu 610039, China)

Abstract: In order to enhance the degree of "decentralization" of the consensus mechanism for Delegated Proof-of-Stake (DPoS) in the blockchain public chain system and to increase the enthusiasm of nodes to vote, an improvement scheme has been proposed. Firstly, the PoW "mining" mechanism based on computing power competition is used to select the set of "agent nodes" and the upper limit of the node's stake is set, and then the set of "consensus nodes" is selected via the voting mechanism, so that the consensus node's election process is more fair in the DPoS mechanism; meanwhile, verifiable random function is introduced to optimize the block generation sequence of consensus nodes, which increases the cost of nodes doing evil, preventing "collusion attacks" by malicious nodes. Secondly, the rewards obtained by the block-producing nodes is rationally distributed using the Shapley value calculation method in game theory, to promote the enthusiasm of the nodes to vote. Finally, credit points are introduced to judge the behavior of nodes, and combined with the current voting rights and block rewards obtained, the comprehensive reputation value (PCredit) is calculated, and then the nodes participating in the consensus in each round are dynamically adjusted through PCredit, which enhances the degree of "decentralization". The experimental results show that the stability and security of the system is enhanced by using the improved DPoS consensus mechanism, and the competition for bookkeeping rights is balanced with ensuring the block rate of nodes.

Key words: blockchain; delegate proof of stake; verifiable random function; game theory; Shapley value