基于权力指数的 DPoS 共谋攻击检测与预防

付晓东[1,2]，漆鑫鑫[1]，刘骊[1]，彭玮[1]，丁家满[1]，代飞[3]

（1. 昆明理工大学信息工程与自动化学院，云南 昆明 650500；
2. 昆明理工大学云南省计算机应用技术重点实验室，云南 昆明 650500；
3. 西南林业大学大数据与智能工程学院，云南 昆明 650224）

摘 要：针对 DPoS 共识机制存在恶意节点通过共谋操纵选举，导致 DPoS 共识过程中区块链安全性无法保证的问题，提出基于权力指数的 DPoS 共谋攻击检测与预防方法。首先，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，以分析恶意节点的行为动机。然后，通过异常的权力指数变化幅度进行攻击检测，在预防 DPoS 共谋攻击的过程中，加入 Softsign 激活函数抑制恶意节点的权力指数。最后，理论分析与实验验证了所提方法检测和预防 DPoS 共谋攻击的有效性。

关键词：区块链；DPoS 共识机制；共谋攻击；权力指数；加权投票博弈

中图分类号：TP309

文献标志码：A

DOI: 10.11959/j.issn.1000−436x.2022233

Detecting and preventing collusion attack in DPoS based on power index

FU Xiaodong[1,2], QI Xinxin[1], LIU Li[1], PENG Wei[1], DING Jiaman[1], DAI Fei[3]

1. Faculty of Information Engineering and Automation, Kunming University of Science and Technology, Kunming 650500, China
2. Yunnan Provincial Key Laboratory of Computer Technology Application, Kunming University of Science and Technology, Kunming 650500, China
3. College of Big Data and Intelligent Engineering, Southwest Forestry University, Kunming 650224, China

Abstract: Since malicious nodes may manipulate voting elections through collusion attacks in consensus mechanism of DPoS, the security of block chain can not be guaranteed in the consensus process of DPoS. To deal with the problem, a method for detecting and preventing collusion attack in DPoS based on power index was proposed. Firstly, a weighted voting game model of DPoS was constructed based on the idea of power index in game theory, and the behavioral motivation of the malicious node could be analyzed. Then, the attacks were detected based on changing range of abnormal power index. During the process of preventing collusion attacks in DPoS, the Softsign activation function was adapted to suppress the power index of malicious nodes. Lastly, the effectiveness of the proposed method to detect and prevent collusion attacks in DPoS was verified through theoretical analysis and experiments.

Keywords: blockchain, DPoS consensus mechanism, collusion attack, power index, weighted voting game

0 引言

2008 年，中本聪提出一种 P2P 形式的加密货币——比特币[1]。比特币出现之后，其底层区块链技术便迅速引起了学术界与各个行业的关注。区块链技术因具有去中心化、难以篡改、集体维护等特

收稿日期：2022−08−12；**修回日期**：2022−10−30

基金项目：国家自然科学基金资助项目（No.61962030, No.62262036）；云南省中青年学术和技术带头人后备人才培养计划基金资助项目（No.202005AC160036）；云南省窦万春专家工作站基金资助项目（No.202105AF150013）；云南省重大科技专项计划基金资助项目（No.202102AD080002）

Foundation Items: The National Natural Science Foundation of China (No.61962030, No.62262036), The Yunnan Provincial Foundation for Leaders of Disciplines in Science and Technology (No.202005AC160036), The Foundation of Dou Wanchun Expert Workstation of Yunnan Province (No.202105AF150013), Major Science and Technology Project of Yunnan Province (No.202102AD080002)

点广泛应用于金融、物联网、交通等领域[2-3]。共识机制[4]作为区块链的重要组成部分，其性能的好坏直接影响区块链系统的安全性、事务处理能力以及可扩展性。然而，由于区块链技术结构的复杂性以及缺乏安全管控，针对区块链系统共识机制层面的攻击也在逐年增加[5-6]。

区块链中常见的共识机制有工作量证明（PoW, proof of work）[7]、权益证明（PoS, proof of stake）[8-9]和委托权益证明（DPoS, delegate proof of stake）[10]等。比特币采用 PoW 的共识机制，通过节点“挖矿”来竞争记账权。虽然 PoW 算法简单且容易实现，但是它在通过“挖矿”达成共识的过程中需要消耗大量计算资源[11]。为了解决 PoW 资源浪费的问题，PoS 被提出[9]。由于 PoS 在一定程度上缩短了达成共识的时间，而且不再需要消耗大量资源，因此 PoS 一经提出就引起广泛关注。虽然 PoS 可避免资源浪费，但是达成共识的过程容易产生垄断，并面临币龄累计攻击[12]、51%攻击[13-14]以及无利害攻击[15]等各种不同攻击的风险。为了解决 PoS 中参与验证与记账的节点数量过多的问题，DPoS 被提出，共识时间进一步缩短，被以太坊[16]、EOSIO[17]等平台作为共识机制。然而，与 PoS 类似，DPoS 依然存在易被攻击的问题。

DPoS 作为 PoS 共识机制的衍生体，其核心在于拥有权益的节点通过投票选出 k 个委托节点，每轮选举结束就由这 k 个节点轮流生成区块，DPoS 共识机制模型如图 1 所示。由于 DPoS 节点的投票权重不同，该投票过程本质上是加权投票，与 PoS 相比，DPoS 减少了共识时间以及资源的消耗。虽然 DPoS 对 PoW 和 PoS 存在的问题进行了改进，但 DPoS 在投票过程中可能存在恶意节点与其他节点串通并选择傀儡委托节点的共谋行为，这种行为也被称为共谋攻击[18]。共谋攻击使恶意节点可操纵选举，被操纵选举出的委托节点会进一步影响共识结果，降低 DPoS 区块链系统的安全性。考虑到目前的研究没有解决 DPoS 共识机制遭受共谋攻击的问题，本文提出了一种基于权力指数（PI, power index）的 DPoS 共谋攻击检测与预防方法来解决上述问题。本文主要贡献如下。

1) 针对 DPoS 中共谋攻击的特点，建立加权投票博弈模型并借鉴博弈理论[19]中的权力指数[20]，分析共谋攻击存在的可能性以及恶意节点发起共谋的行为动机。通过计算各个节点在投票过程中的权力指数值，得到每个节点对选举结果影响程度的大小。

2) 对 DPoS 中共谋攻击进行检测与预防。由于恶意节点在加权投票博弈过程中权力指数可能出现异常，可以根据权力指数变化幅度判别投票节点的加权投票博弈中是否存在共谋攻击。为了对 DPoS 中共谋攻击进行预防，本文通过 Softsign 激活函数抑制恶意节点的权力指数，同时抑制恶意节点的行为动机。

3) 对权力指数的单调性以及 Softsign 函数的饱和性进行理论证明，验证了 DPoS 存在共谋攻击以及攻击预防方法的合理性。实验验证了 DPoS 中共谋攻击存在的合理性，以及 DPoS 共谋攻击检测与预防方法的有效性与优越性。

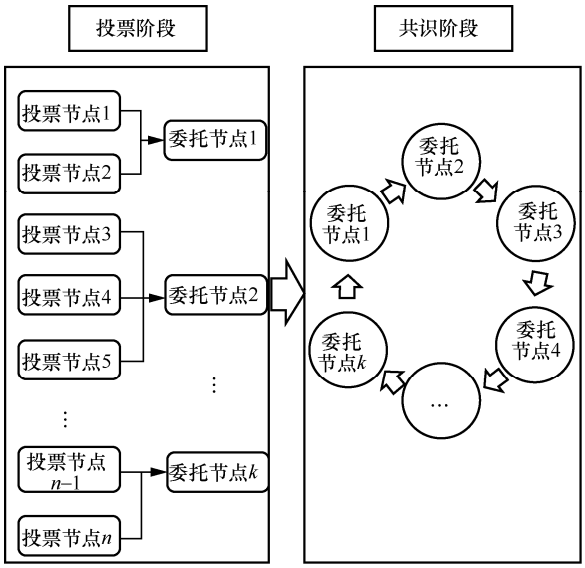

图 1 DPoS 共识机制模型

1 相关工作

近年来，为了提高区块链共识层面的安全性，国内外学者展开了一系列的研究。针对非 DPoS 区块链系统的研究中，Yang 等[21]提出了一种将矿工历史加权信息与计算难度相结合的方案，以缓解 PoW 中 51%攻击。为了减轻 PoS 中的远程攻击，AlMallohi 等[22]提出了一种在区块链技术中实施检查点的方法。本文将提高 DPoS 区块链系统安全性的相关研究分为理论与策略分析和共识机制的改进研究 2 个层面。

为了对 DPoS 的安全问题进行理论与策略分析，Wang 等[23]提出了一种 DPoS 的博弈分析方法。该方法通过构建扩展的 DPoS 博弈树，理论上可以

有效地分析是否存在恶意攻击。田国华等[24]根据区块链层次结构对现有的区块链攻击进行分类，并针对已知的区块链系统设计了各种攻击和防御手段。魏松杰等[25]以比特币与以太坊为例，对区块链系统的安全威胁进行分类和总结。

针对DPoS中投票选举的中心化问题，Luo等[26]提出了一种 DPoS 共识机制选举算法，该算法改进了基于环的协调器选举算法，不仅降低了交易成本，而且达到了杜绝垄断和去中心化的效果。Yao等[27]在 DPoS 委托节点的选择阶段通过节点分组实现了组间隔离，提高了选择过程中委托节点的公平性；此外，该研究利用鱼群算法提高了区块链网络的安全性能和容错率。为了提高 DPoS 节点投票的积极性，Wang 等[28]提出一种基于聚类算法的激励机制，由于传统的聚类算法存在需要预测聚类数量、无法处理异常值等问题，该研究还提出一种 Hegselmann-Krause 意见动力学聚类算法来满足奖励分配机制的需求。

通过对目前的 DPoS 共识机制的安全研究进行分析可以看到，一方面，现有研究主要以理论分析为主对 DPoS 面临的各种恶意攻击进行梳理，总结出 DPoS 共识机制遭受的各种攻击的基本原理，提出一些建议与防御措施，但这种理论分析缺乏具体的实验加以验证。另一方面，现有研究主要利用特殊方法与技术对 DPoS 进行改进，激励节点的投票积极性以及隔绝恶意节点的攻击行为。然而，DPoS 共识机制的关键在于如何保证委托节点选举的安全性。一旦委托节点的选举过程被操纵，DPoS 共识机制的安全性与一致性也就无法保证。虽然部分文献提出了新的选举算法，但未验证针对 DPoS 的共谋攻击进行检测与预防的有效性。而且，以上研究都没有对 DPoS 的共谋攻击行为进行分析。考虑到博弈中的个体理性，应通过建立分析模型并找到恶意节点的行为动机解决 DPoS 中面临共谋攻击的问题。针对上述研究中没有考虑到的问题以及不足，本文提出了一种基于权力指数的 DPoS 共谋攻击检测与预防方法，通过建立加权投票博弈模型对恶意节点的行为动机进行分析。同时，根据分析结果对 DPoS 中的共谋攻击进行检测与预防，最终提高 DPoS 区块链的安全性。

2　DPoS 共谋攻击的检测与预防

权力指数是加权投票博弈中衡量个体影响博弈结果能力的指标。目前，Shapley-Shubik[29-30]和 Banzhaf[29,31]权力指数是加权投票博弈较常见的 2 个权力指数。Shapley-Shubik 权力指数的核心是将沙普利值应用于投票领域，其主要思想是计算某一特定个体对任意联盟的价值的期望贡献。Banzhaf 权力指数是在所有联盟出现概率相同的情形下，计算某一特定个体对任何联盟的平均边际贡献。权力指数的值越大，特定个体影响投票结果的能力就越大。

考虑到 DPoS 委托节点的选举就是通过加权投票得到的，本文将 Shapley-Shubik 与 Banzhaf 权力指数作为 DPoS 投票节点在加权投票博弈中影响委托节点选举结果能力的指标。由于 DPoS 中的共谋攻击就是恶意节点串通其他节点合并成串通同盟的过程，且在存在恶意节点的博弈中，恶意节点会从自身成本角度出发，逐步从小权重节点开始共谋。串通同盟形成过程将导致在同一加权投票博弈中的最小权重且不参与共谋的节点的权力指数变化与不存在恶意节点的博弈中最小权重且不参与共谋的节点的权力指数变化不同。因此，可根据异常的权力指数变化对 DPoS 加权投票中的共谋攻击进行检测。此外，为了预防 DPoS 中的共谋攻击，本文使用 Softsign 激活函数在检测过程中对恶意节点的共谋攻击行为进行惩罚。为更清晰地阐述本文方法，表 1 展示了本文方法涉及的符号及其含义。

表 1　　符号及其含义

符号	含义
k	DPoS 中的委托节点数量
N	DPoS 中的投票节点集合（它的每个非空子集被称为联盟，$\|N\|$ 表示联盟中的个体数量，这里 $\|N\|=n$）
nd	DPoS 中的投票节点
n	DPoS 中的投票节点数量
W	DPoS 中的投票节点对应的权重集合
w	DPoS 中的投票节点对应的权重
v	伴随可转移的价值函数
q	加权投票博弈的阈值
(N,W,q,v)	DPoS 中的一个加权投票博弈，其中 (N_k,W_k,q_k,v_k) 表示第 k 个加权投票博弈
SSI	Shapley-Shubik 权力指数
PBI	Banzhaf 权力指数
M_k	第 k 个加权投票博弈中最小权重且不参与共谋的节点的权力指数变化幅度

2.1 DPoS 的加权投票博弈

假设 DPoS 在投票过程中有 n 个投票节点 $N=\{\mathrm{nd}_1,\mathrm{nd}_2,\cdots,\mathrm{nd}_n\}$，投票节点根据币龄通过最小值化公式进行等比缩小，当缩小到最小投票节点的币龄为正整数 1 时，再全部取整转成权重集合 $W=\{w_1,w_2,\cdots,w_n\}$ 进行加权投票。加权投票博弈是投票领域的一种联盟博弈[32]形式，所以，DPoS 中的加权投票博弈可以看成一个简单的联盟博弈的扩展。定义四元组 (N,W,q,v) 为 DPoS 的一个加权投票博弈，其中价值函数 v 具体描述为当联盟 S 的权重达到或者超过阈值 q 时，联盟 S 获胜，即

$$v(S)=\begin{cases}1,\sum\limits_{i\in S}w_i\geqslant q\\0,\text{其他}\end{cases}\tag{1}$$

2.2 DPoS 中 Shapley-Shubik 与 Banzhaf 权力指数

由于 Shapley-Shubik 权力指数反映的是投票个体在包含其联盟中的平均力量，仅反映了个体对联盟的影响。而 Banzhaf 权力指数只从联盟的角度考虑，投票个体的“权力”是其作为获胜联盟中关键加入者的个数。总而言之，虽然 2 个权力指数都能反映投票个体在群体决策中的实际权力，但其中任何一个权力指数都无法从多个角度完整反映出个体对投票结果的实际影响能力值。为了能更好地分析 DPoS 共谋攻击中各个投票节点在多个角度下实际权力的变化，本文结合 Shapley-Shubik 与 Banzhaf 权力指数对 DPoS 共谋攻击进行检测和防范。

根据 Shapley-Shubik 权力指数计算的基本原理，假设包含节点 i 的投票节点集合为一个联盟，且该联盟规模为 $|S|\in[1,n]$，所有不同规模的联盟形成的概率相同，一个特定规模的联盟出现概率为 $\frac{1}{n}$。为了构建一个包含节点 i 且规模为 $|S|$ 的联盟，只能从剩下的 $n-1$ 个节点中选择 $|S|-1$ 个节点组成。根据上述逻辑进行排列组合的计算可以得到 $\mathrm{C}_{n-1}^{|S|-1}$，而 $\mathrm{C}_{n-1}^{|S|-1}$ 的倒数是任意一个包含节点 i 的联盟形成的概率。将 $\mathrm{C}_{n-1}^{|S|-1}$ 的倒数与 $\frac{1}{n}$ 相乘，可得到形成特定规模为 $|S|$ 的联盟包含节点 i 的概率。用 $v(S)-v(S\setminus\{i\})$ 表示节点 i 为联盟 S 做出的边际贡献。根据上述对 Shapley-Shubik 权力指数的描述，对 DPoS 投票节点的 Shapley-Shubik 权力指数的计算定义如下。

n 维向量 $\mathbf{SSI}(N,W,q,v)=\left(\mathrm{SSI}_{\mathrm{nd}_1}(N,W,q,v),\cdots,\mathrm{SSI}_{\mathrm{nd}_n}(N,W,q,v)\right)$ 为 DPoS 投票节点在加权投票博弈 (N,W,q,v) 的 n 个 Shapley-Shubik 权力指数，其中，第 i 个 DPoS 节点的 Shapley-Shubik 权力指数为

$$\begin{aligned}&\mathrm{SSI}_{\mathrm{nd}_i}(N,W,q,v)=\\&\sum_{S\subseteq N|i\in S}\frac{1}{\mathrm{C}_{n-1}^{|S|-1}}\frac{1}{n}\left[v(S)-v\left(S\setminus\{i\}\right)\right]=\\&\sum_{S\subseteq N|i\in S}\frac{(|S|-1)!(n-|S|)!}{n!}\left[v(S)-v\left(S\setminus\{i\}\right)\right]\end{aligned}\tag{2}$$

根据 Banzhaf 权力指数的计算定义，假设所有联盟出现概率相同，除去节点 i，其他投票节点加入节点 i 的联盟的概率为 $\frac{1}{2}$，则所有联盟出现的概率是 $\frac{1}{2^{n-1}}$。为了得到节点 i 对所有联盟的平均边际贡献，本文对 DPoS 投票节点的 Banzhaf 权力指数的计算定义如下。

n 维向量 $\mathbf{PBI}(N,W,q,v)=\left(\mathrm{PBI}_{\mathrm{nd}_1}(N,W,q,v),\cdots,\mathrm{PBI}_{\mathrm{nd}_n}(N,W,q,v)\right)$ 为 DPoS 投票节点在加权投票博弈 (N,W,q,v) 的 n 个 Banzhaf 权力指数，其中，第 i 个 DPoS 节点的 Banzhaf 权力指数为

$$\begin{aligned}&\mathrm{PBI}_{\mathrm{nd}_i}(N,W,q,v)=\\&\frac{1}{2^{n-1}}\sum_{S\subseteq N|i\in S}[v(S)-v(S\setminus\{i\})]\end{aligned}\tag{3}$$

2.3 基于 PI 的 DPoS 共谋攻击检测

一个加权投票博弈只能讨论和分析 DPoS 在投票过程中选出一位委托节点的情况下是否存在共谋攻击。然而，DPoS 在加权投票阶段会选择 k 个委托节点。因此，本文在 k 个加权投票博弈下对 DPoS 共谋攻击进行分析与检测。

在加权投票博弈中，恶意节点为了形成新的恶意节点会串通投票过程中权重较小的节点，导致攻击发起后最小权重且不参与共谋的节点发生改变。根据分析过程中的多次模拟，可以计算 DPoS 恶意节点在共谋攻击发起前后的最小权重且不参与共谋的节点的权力指数的变化幅度，进而得到 DPoS 在 k 个加权投票博弈中检测存在共谋攻击的范围。如果一个加权投票博弈的变化幅度在设置的范围内，则认定加权投票博弈中存在恶意节点的共谋攻击。为了对检测效果进行具体评估，本文共谋攻击检测的对比实验将在相同条件下通过皮尔逊相关系数比较不同方法得到测试值。

设 M_k 是第 k 个加权投票博弈中最小权重且不参与共谋的节点的权力指数变化幅度，由计算最小权重且不参与共谋的节点中 2 个权力指数变化幅度的均值获得。$\widetilde{\mathrm{SSI}}(N_k,W_k,q_k,v_k)$ 和 $\widetilde{\mathrm{PBI}}(N_k,W_k,q_k,v_k)$ 是第 k 个加权投票博弈中最小权重且不参与共谋的节点在攻击发起后的 Shapley-Shubik 和 Banzhaf 权力指数。$\widehat{\mathrm{SSI}}(N_k,W_k,q_k,v_k)$ 和 $\widehat{\mathrm{PBI}}(N_k,W_k,q_k,v_k)$ 是攻击发起前的 2 个权力指数。定义 M_k 为

$$M_k=\frac{1}{2}\left(\frac{\widetilde{\mathrm{SSI}}(N_k,W_k,q_k,v_k)}{\widehat{\mathrm{SSI}}(N_k,W_k,q_k,v_k)}+\frac{\widetilde{\mathrm{PBI}}(N_k,W_k,q_k,v_k)}{\widehat{\mathrm{PBI}}(N_k,W_k,q_k,v_k)}\right) \tag{4}$$

为了对 k 个加权投票博弈分区中存在的共谋攻击进行统计，设 M^{l} 与 M^{h} 分别是存在恶意节点的加权投票博弈中最小权重且不参与共谋的节点的权力指数最小值与最大值的变化幅度，$D_k(M_k)$ 为第 k 个加权投票博弈中是否存在共谋攻击的结果。如果存在，结果为 1，否则为 0，即

$$D_k(M_k)=\begin{cases}1, M^l\leqslant M_k\leqslant M^h\\ 0, \text{其他}\end{cases} \tag{5}$$

同时，设定 m 维向量 $\boldsymbol{D}=(D_1,D_2,\cdots,D_m)$，其中 D_m 为 k 个加权投票博弈中存在 DPoS 共谋攻击的加权投票博弈分区数量，即

$$D_m=\sum_{j=1}^{k}D_j(M_j) \tag{6}$$

2.4　基于 Softsign 激活函数的 DPoS 共谋攻击预防

基于权力指数对 DPoS 共谋攻击进行检测的最终目的是对面临的攻击进行预防。为了抑制恶意节点在形成恶意攻击同盟过程中权力指数的增加，本文采用 Softsign 激活函数作为恶意节点的抑制函数。激活函数常用于神经网络[33]中神经元输入端映射到输出端的函数，可分为饱和的激活函数与非饱和的激活函数。其中，饱和的激活函数是指随着输入值 x 的不断增加，输出值 y 逐渐不再变化。目前，较常见的饱和的激活函数有 Softsign、Sigmoid 和 Tanh 等。由于 Softsign 激活函数的饱和性质可以降低恶意节点通过串通其他节点以大幅增长其权力指数的可能性，以及该激活函数的抑制效果相比 Sigmoid 和 Tanh 更加显著，因此本文选择在检测 DPoS 共谋攻击的阶段加入 Softsign 激活函数对恶意节点的同盟进行抑制，即在共谋攻击发起过程中，如果恶意节点在检测的时候被识别，其同盟不断增加的权重通过 Softsign 激活函数进行饱和计算，使恶意节点串通同盟的权重趋于定值，最终其权力指数也将被抑制，恶意节点无法操纵选举结果会使其行为动机被削弱，最终对 DPoS 共谋攻击达到预防的效果。假设 w_c 为恶意节点串通同盟 $C\subseteq N$ 的权重，定义 Softsign 激活函数为

$$w_c=\sum_{i\in C}w_i \tag{7}$$

$$\mathrm{Softsign}(w_c)=\frac{w_c}{1+|w_c|} \tag{8}$$

3　基于 PI 的 DPoS 共谋攻击检测与预防理论分析

本节通过权力指数的合并单调性[29,34]对 DPoS 共谋攻击的存在合理性进行证明；同时，通过 Softsign 激活函数的饱和性对预防 DPoS 共谋攻击的有效性进行证明。

性质 1　Shapley-Shubik 权力指数的单调性。当 q 不变时，给定一个 DPoS 的加权投票博弈 (N,W,q,v)，节点 $i,j\in S'$ 以及联盟 $S'\subseteq N$，有 $\mathrm{SSI}_{\mathrm{nd}_{i\cup j}}(N,W,q,v)>\mathrm{SSI}_{\mathrm{nd}_i}(N,W,q,v)$。

证明　详见附录 1。

性质 2　Banzhaf 权力指数的单调性。当 q 不变时，给定一个 DPoS 的加权投票博弈 (N,W,q,v)，节点 $i,j\in S'$ 以及联盟 $S'\subseteq N$，有 $\mathrm{PBI}_{\mathrm{nd}_{i\cup j}}(N,W,q,v)>\mathrm{PBI}_{\mathrm{nd}_i}(N,W,q,v)$。

证明　详见附录 1。

根据性质 1 与性质 2，DPoS 中恶意节点发起共谋攻击的动机在于利用权力指数的合并单调性提升自身对选举结果的影响力，最终达到操纵选举的目的。换句话说，DPoS 共谋攻击的存在是合理的。同时，权力指数的合并单调性使在 DPoS 恶意节点发起共谋攻击的过程中可以找到异常权力指数变化值，从而通过异常变化值可检测 DPoS 中的共谋攻击。

性质 3　Softsign 激活函数的饱和性。

证明　详见附录 1。

根据性质 3，在恶意节点串通同盟的权重不断增加的过程中，由于 Softsign 激活函数的饱和性，恶意节点串通同盟的权重最后趋于不再变化的值，从而使其权力指数不再增加。

总而言之，本文通过理论证明权力指数的合并单调性，直观地分析出恶意节点发起 DPoS 共谋攻击的动机，即恶意节点可通过共谋攻击提高权力指数来操纵投票选举。同时，计算出存在共谋攻击博弈与不存在共谋攻击博弈中权力指数的不同变化幅度值，最终通过存在共谋攻击的博弈的异常权力指数变化幅度，有效检测出 DPoS 中的共谋攻击。最后，基于 Softsign 激活函数的饱和性，在 DPoS 遭受共谋攻击的过程中抑制恶意节点串通同盟的权力指数，以起到预防该攻击的效果。

4 实验研究与分析

为验证本文基于 PI 的 DPoS 共谋攻击检测与预防方法的有效性，设计了相关实验。实验环境为 Windows10 操作系统、Core i7-11700k 处理器、16 GB 内存，开发环境为 PyCharm 2021，编程语言为 python 3。

由于随机模拟节点权重等相关数据进行实验不能保证实验结果的真实性，本文采用公开的 X-block 数据集[35-36]。该数据集包含被标记的以太坊节点的隐私数据以及节点间的交易数据。被标记的以太坊节点的隐私数据有 2 880 个节点，节点的隐私数据包含物理地址、钱包余额等敏感信息。而节点间的交易数据包含几十万条以太坊节点间的历史交易数据。

根据以太坊的隐私数据，实验将其中各个节点的币龄通过最小值化以及取整，转换成各个节点的权重，最后将得到的权重来模拟 DPoS 加权投票博弈中共谋攻击的过程。考虑到基于支持向量机的方法可以有效识别及检测类似共谋攻击，且文献[37]将支持向量机的检测方法 OSVM（one class support vector machine）融入自选异常数据检测的算法中对 DPoS 中恶意节点的自私行为进行识别检测，以提高 DPoS 的安全性。因此，本节通过以太坊的节点数据，将本文方法与基于支持向量机的检测方法进行对比实验。而在 DPoS 共谋攻击的预防实验中，为了显示 Softsign 激活函数的抑制效果的优越性，对 Sigmoid 以及 Tanh 激活函数在检测过程中的抑制结果进行对比验证。

4.1 DPoS 共谋攻击分析实验

根据第 3 节对权力指数的相关定义可知，节点权力指数越大，其对加权投票博弈选举结果的影响力也就越大。因此，本文在选出 k 个委托节点的加权投票过程中，用权力指数得到恶意节点发起共谋攻击过程中的变化值。由于 DPoS 区块链系统一般会选出 k=21 个委托节点，本文对 21 个不同的加权投票博弈进行实验。此外，按照总权重递增的顺序模拟了 DPoS 区块链中选出 21 个委托节点的难度。本文实验将 2 880 个以太坊节点分成 21 个博弈分区。为了得到合理的分析结果，本文实验在这些加权投票博弈中随机选择权重相同的恶意攻击节点。同时，由于恶意节点发起共谋攻击时其本身的权重未知，不同权重的攻击者在发起共谋攻击时，恶意节点联盟的形成过程不同，而不同的过程将影响最终结果的判断，为了能够在不同权重下合理分析出攻击者的行为动机，本文将攻击者权重大于博弈中投票节点的平均权重的类型定义为较大权重的攻击者，反之，则为较小权重的攻击者。图 2 为恶意节点有较大权重时，共谋攻击发起前后的 2 个权力指数。图 3 为恶意节点有较小权重时，共谋攻击发起前后的 2 个权力指数。图 2 与图 3 中的 SSI-B 与 SSI-A 表示恶意节点发起共谋攻击前后的 Shapley-Shubik 权力指数，PBI-B 与 PBI-A 表示攻击发起前后的 Banzhaf 权力指数。

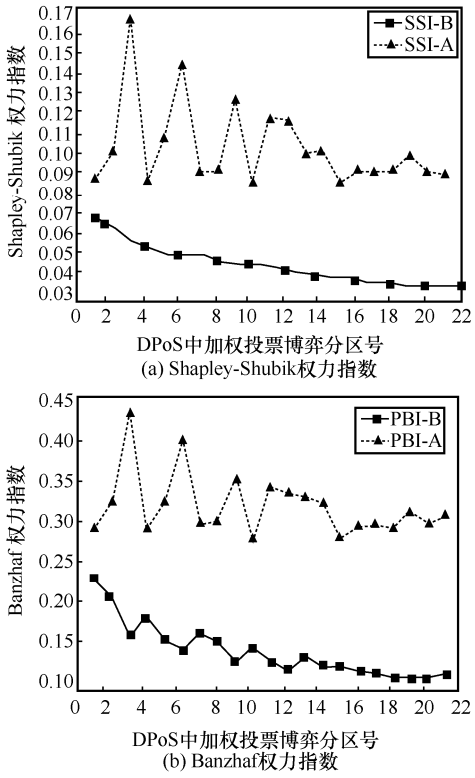

图 2 恶意节点有较大权重时，共谋攻击发起前后的 2 个权力指数

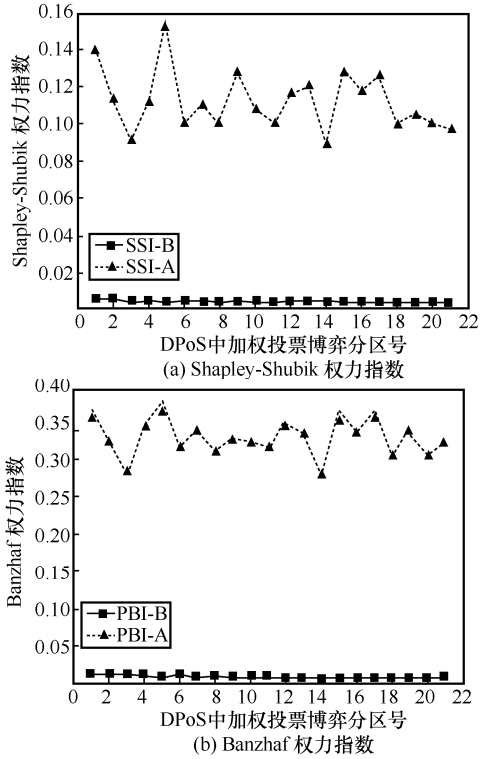

图 3　恶意节点有较小权重时，共谋攻击发起前后的 2 个权力指数

由图 2 与图 3 可知，恶意节点发起攻击之后，与其他节点共谋并形成一个权重较大且新的恶意节点，增加了恶意节点对联盟的贡献，这使它发起攻击后的 Shapley-Shubik 与 Banzhaf 权力指数的曲线都在它发起攻击前的 2 个权力指数的曲线之上。同时，无论发起共谋攻击的恶意节点的权重多大，恶意节点的 Shapley-Shubik 与 Banzhaf 权力指数在发起共谋攻击之后都会增加。此外，恶意节点权力指数增加就是恶意节点通过串通攻击前的其他节点增加了恶意节点对获胜联盟的影响，是导致其权力指数增加的主要原因。也就是说，恶意节点可以通过共谋并吸收其他节点权重增加其在加权投票博弈中的权力指数，实现操纵投票选举。同时，从恶意节点的个体理性的角度证实了 DPoS 中共谋攻击存在的可能性，恶意节点发起攻击后，其 2 个权力指数的增加也从侧面证明了权力指数的合并单调性。

从图 2 和图 3 还能看到，随着加权投票博弈的总权重增加，恶意节点在共谋攻击发起前的 Shapley-Shubik 权力指数相比 Banzhaf 权力指数更加具有单调性，即恶意节点发起共谋攻击前的 Shapley-Shubik 权力指数逐渐变小。从 Shapley-Shubik 权力指数的角度上讲，由于恶意攻击节点越想操纵加权投票博弈分区序号越大的选举，就越会降低恶意节点在总权重较大博弈分区中的影响力，其操纵的难度就会越大。总而言之，恶意节点可通过提高本身的权力指数形成有效的共谋攻击。

4.2　DPoS 共谋攻击检测实验

为了验证本文 DPoS 共谋攻击检测方法的性能，将实验分成横向参照对比和方法对比两类。其中，横向参照对比是通过在 21 个 DPoS 的加权投票博弈中随机设定存在共谋攻击博弈分区，然后通过本文方法检测的结果与设定值比较。方法对比是通过皮尔逊相关系数对比本文方法与 OSVM 方法的检测效果。

由于在 21 个加权投票博弈中设定存在共谋攻击的博弈数量过少，无法充分证明本文检测方法的具体效果；设定的博弈数量过多，将导致在获取相同利益的前提下攻击成本上升，不符合恶意节点从个体理性出发的利益需求。因此，在横向参照对比的实验中，本文通过设定 5 组不同数量且存在共谋攻击的博弈分区来展示检测结果，且检测结果进行多次实验求平均值，如图 4 所示。从图 4 中可知，无论恶意节点的类型如何，5 组存在共谋攻击的博弈分区的设定值与本文方法检测的测试值没有太大区别。

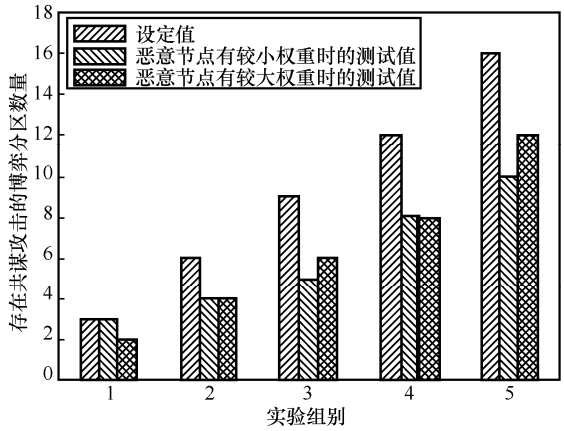

图 4　横向参照对比检测

虽然图 4 的结果表明本文方法的检测效果不错，但缺乏其他方法检测 DPoS 共谋攻击的结果对比，因此仍然需要相关指标进行方法对比。OSVM 方法的实验数据是从几十万条以太坊的历史节点交易数据中随机选择 5 000 条数据分别作为两类恶意节点类型的训练集。设定 m 维向量 $\boldsymbol{A}=(A_1,A_2,\cdots,A_m)$，其中，$A_m$ 为设定的 k 个加权投票博弈中存在 DPoS 共谋攻击的加权投票博弈数量。如果检测方法得到的检测值 A_m 越接近设定存在

共谋攻击的加权投票博弈数量值 D_m，则说明检测效果越好。皮尔逊相关系数、欧几里得距离以及余弦相似度经常用于度量 2 个变量之间的相关性，当变量是多维向量时，皮尔逊相关系数比欧几里得距离更能展示向量间的运动趋势，且与余弦相似度相比，其能弥补在维度计算上的缺陷。所以，为了突出本文方法的优越性，本文将皮尔逊相关系数作为方法间的检测指标。根据皮尔逊相关系数的定义，本文方法的皮尔逊相关系数 PI_PCC 为

$$\mathrm{PI\_PCC}(A,D)=\frac{\sum_{f=1}^{m}\left(\left(A_f-\bar{A}\right)\left(D_f-\bar{D}\right)\right)}{\sqrt{\sum_{f=1}^{m}\left(A_f-\bar{A}\right)^2}\sqrt{\sum_{f=1}^{m}\left(D_f-\bar{D}\right)^2}} \tag{9}$$

其中，$\bar{A}$ 为 $\boldsymbol{A}$ 向量元素的平均值，$\bar{D}$ 为 $\boldsymbol{D}$ 向量元素的平均值。

利用皮尔逊相关系数，在不同维度上对本文基于 PI 方法以及文献[37]中 OSVM 方法的检测效果如图 5 所示。

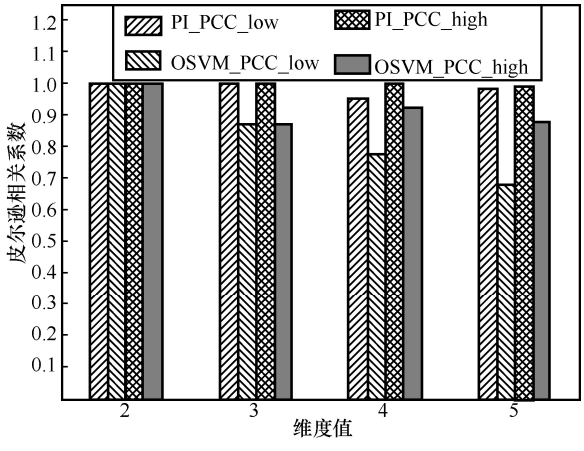

图 5 检测方法对比

图 5 中， PI_PCC_low 与 OSVM_PCC_low 表示在恶意节点有较小权重时，本文方法和 OSVM 方法得到的皮尔逊相关系数；PI_PCC_high 与 OSVM_PCC_high 表示在恶意节点有较大权重时，2 种方法得到的皮尔逊相关系数。基于皮尔逊相关系数的性质可知，其值越接近 1，2 个向量越呈正相关。从图 5 的结果可知，不管恶意节点的类型如何，基于 PI 的 DPoS 共谋攻击检测的皮尔逊相关系数总是不小于 OSVM 方法，也就是说，本文方法的检测效果优于 OSVM 方法。

4.3 DPoS 共谋攻击的预防实验

通过 DPoS 共谋攻击分析与检测实验可知，恶意节点主要通过增加自身的权力指数来操纵 DPoS 中的投票选举。为了显示 Softsign 激活函数在 DPoS 共谋攻击环境下对恶意节点权力指数的抑制效果，本文使用 Sigmoid 以及 Tanh 激活函数进行 DPoS 共谋攻击的预防实验。为了和上述实验保持一致性，预防实验同样在 2 种不同类型的恶意节点下进行。同时，实验从 21 个 DPoS 的加权投票博弈中随机选择在检测出共谋攻击的博弈分区中加入激活函数并计算加入激活函数前后的权力指数的变化。最后，对这些博弈分区的权力指数平均值，本文将 Sigmoid 以及 Tanh 激活函数作为对比，图 6 与图 7 具体展示了加入 3 种激活函数下，恶意节点有较大权重和较小权重时的 2 个权力指数的变化情况。

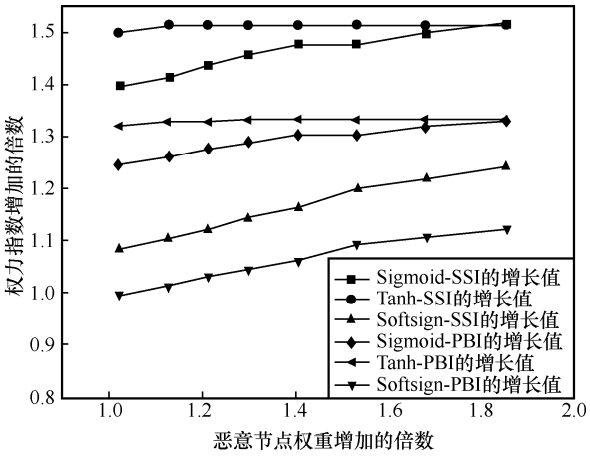

图 6 恶意节点有较大权重时，加入激活函数后的 2 个权力指数

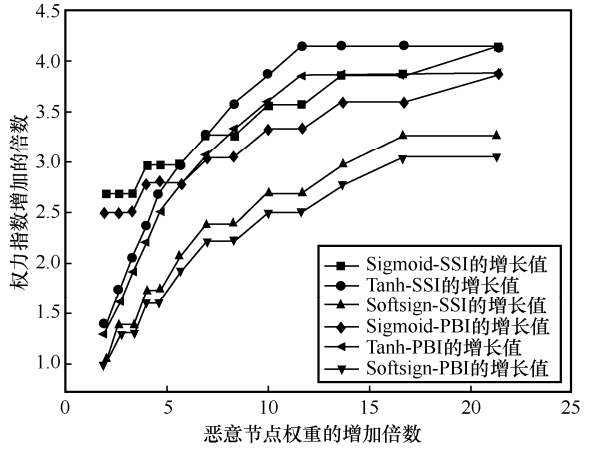

图 7 恶意节点有较小权重时，加入激活函数后的 2 个权力指数

由图 6 可以看出，当恶意节点有较大权重时，Sigmoid 与 Tanh 激活函数的曲线比较相近，也就是

说，这 2 个激活函数在抑制恶意节点的效果方面相差不大。但是，与 Softsign 激活函数相比，Sigmoid 和 Tanh 激活函数的曲线都在 Softsign 激活函数的上方，即 Softsign 激活函数的抑制效果明显更好。

此外，之前的实验表明，当恶意节点有较小权重且未加入激活函数时，恶意节点的权力指数增加了十倍甚至几十倍。而加入 Softsign 激活函数后，图 7 中恶意节点权力指数增加的倍数最多不超过 3.5 倍。而且从图 7 可知，当恶意节点有较小权重时，相比 Tanh 激活函数，Softsign 激活函数的曲线变化更频繁，表明 Softsign 激活函数值的收敛比 Tanh 激活函数值的更慢，但由于 Softsign 激活函数的曲线一直在其他曲线下方，说明其在抑制效果方面仍然比 Tanh 激活函数要好。

图 8 展示了加入 Softsign 激活函数前后，检测存在共谋攻击的博弈分区数量。实验结果最终分成恶意节点有较大与较小权重 2 种类型，实验通过比较加入 Softsign 激活函数前后检测出 DPoS 中存在共谋攻击的博弈分区数量，展示恶意节点的抑制效果。从图 8 可知，加入 Softsign 激活函数后，检测存在共谋攻击的博弈分区不超过 2 个，说明其能在一定程度上抑制恶意节点在 DPoS 加权投票阶段中的共谋攻击，使恶意节点共谋行为的动机降低，对 DPoS 共谋攻击起到预防效果。

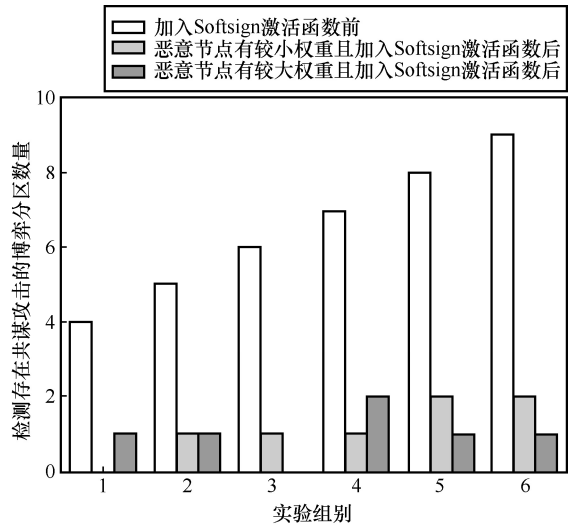

图 8　加入 Softsign 激活函数前后，检测存在共谋攻击的博弈分区数量

5　结束语

本文针对 DPoS 共识机制中恶意节点发起共谋攻击来操纵委托节点的选举导致 DPoS 区块链的安全性无法保证的问题，通过结合博弈理论中加权投票模型以及权力指数，提出了一种基于权力指数的 DPoS 共谋攻击检测与预防方法。首先通过定义权力指数来度量投票节点在加权投票博弈过程中影响结果的能力，接着对权力指数异常变化的恶意节点博弈分区进行 DPoS 共谋攻击检测，然后采用 Softsign 激活函数抑制恶意节点的行为来预防攻击，最后通过理论分析与实验验证了本文方法的合理性与有效性。

现阶段本文采用 Softsign 激活函数虽然可以有效抑制恶意节点的权力指数，但 Softsign 激活函数存在抑制速率较慢的问题。因此，后续研究将继续探索新的 DPoS 共谋攻击预防方法，进一步提升 DPoS 区块链系统的安全性。

附录 1　权力指数的单调性及 Softsign 激活函数的饱和性证明

性质 1 的证明。首先，根据 Shapley-Shubik 权力指数原理与式(2)可得

$$\mathrm{SSI}_{\mathrm{nd}_{i\cup j}}(N,W,q,v)=\sum_{S'\subseteq N|i,j\in S'}\frac{1}{\mathrm{C}_{n-2}^{|S'|-1}}\frac{1}{n-1}\left[v(S')-v\left(S'\setminus\{i,j\}\right)\right]=\sum_{S'\subseteq N|i,j\in S'}\frac{(|S'|-1)!(n-|S'|-1)!}{(n-1)!}\left[v(S')-v\left(S'\setminus\{i,j\}\right)\right]$$

假定节点 i 与节点 j 合并成一个联盟 S'，$|S'|\in[2,n]$。由于各种规模的联盟出现的可能性是相同的，因此特定联盟出现的概率为 $\frac{1}{n-1}$。为了形成一个规模为 $|S'|$ 的联盟，将从剩余 $n-2$ 个节点中选择 $|S'|-1$ 个节点与节点 i、j 组成联盟。这个过程可以看成排列组合 $\mathrm{C}_{n-2}^{|S'|-1}$。由于在计算节点 i 的 Shapley-Shubik 权力指数的过程中，联盟 S 是规模为 $|S|$ 且包含节点 i 的联盟，$|S|\in[1,n]$。当 $|S|=1$ 时，$\mathrm{SSI}_{\mathrm{nd}_i}(N,W,q,v)=\frac{1}{n}$。为了方便比较，式(2)可转换为 $\frac{1}{n}\sum_{S'\subseteq N|i,j\in S'}\frac{(|S'|-1)!(n-|S'|)!}{n!}\left[v(S')-v\left(S'\setminus\{i,j\}\right)\right]$。

最后，$\frac{\mathrm{SSI}_{\mathrm{nd}_{i\cup j}}(N,W,q,v)}{\mathrm{SSI}_{\mathrm{nd}_i}(N,W,q,v)}=n\frac{n}{n-|S'|}>1$，即节点 i、j 合并后 Shapley-Shubik 权力指数增加。

性质 2 的证明。当节点 i 合并节点 j 时，根据 Banzhaf 的计算原理，除去节点 i 与节点 j，可得所有联盟出现的概率 $\frac{1}{2^{n-2}}$ 将大于 $\frac{1}{2^{n-1}}$，最终使 Banzhaf 权力指数增加。

性质 3 的证明。由于节点的权重都为正数，当恶意节点串通同盟的权重 $w_c>0$，对函数 $\frac{w_c}{1+w_c}$ 求导可得 $\frac{1}{(1+w_c)^2}$。随着 w_c 的增加，函数的导数越趋于 0。

参考文献：

[1] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[R]. 2008.

[2] KHAN S N, LOUKIL F, GHEDIRA-GUEGAN C, et al. Blockchain smart contracts: applications, challenges, and future trends[J]. Peer-to-Peer Networking and Applications, 2021, 14(5): 2901-2925.

[3] LIU D X, NI J B, HUANG C, et al. Secure and efficient distributed network provenance for IoT: a blockchain-based approach[J]. IEEE Internet of Things Journal, 2020, 7(8): 7564-7574.

[4] FU X, WANG H M, SHI P C. A survey of Blockchain consensus algorithms: mechanism, design and applications[J]. Science China Information Sciences, 2020, 64(2): 1-15.

[5] JANG J, LEE H N. Profitable double-spending attacks[J]. Applied Sciences, 2020, 10(23): 8477.

[6] NICOLAS K, WANG Y, GIAKOS G C. Comprehensive overview of selfish mining and double spending attack countermeasures[C]//Proceedings of 2019 IEEE 40th Sarnoff Symposium. Piscataway: IEEE Press, 2019: 1-6.

[7] 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.
XIA Q, DOU W S, GUO K W, et al. Survey on blockchain consensus protocol[J]. Journal of Software, 2021, 32(2): 277-299.

[8] 曾诗钦, 霍如, 黄韬, 等. 区块链技术研究综述：原理、进展与应用[J]. 通信学报, 2020, 41(1): 134-151.
ZENG S Q, HUO R, HUANG T, et al. Survey of blockchain: principle, progress and application[J]. Journal on Communications, 2020, 41(1): 134-151.

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

[10] LARIMER D. Delegated proof-of-stake (DPoS)[R]. 2014.

[11] VRIES A D, et al. Bitcoin's growing energy problem[J]. Joule, 2018, 2(5): 801-805.

[12] KING S, NADAL S. PPCoin: peer-to-peer crypto-currency with proof-of-stake[EB]. (2012-08-19) [2022-07-29].

[13] YE C C, LI G Q, CAI H M, et al. Analysis of security in blockchain: case study in 51%-attack detecting[C]//Proceedings of 2018 5th International Conference on Dependable Systems and Their Applications (DSA). Piscataway: IEEE Press, 2018: 15-24.

[14] SHANAEV S, SHURAEVA A, VASENIN M, et al. Cryptocurrency value and 51% attacks: evidence from event studies[J]. SSRN Electronic Journal, 2018: doi.org/10.3905/jai.2019.1.081.

[15] NICOLAS H. It will cost you nothing to ‘kill’ a proof-of-stake crypto-currency[J]. SSRN Electronic Journal, 2014: doi.org/10.2139/ssrn.2393940.

[16] WOOD G. Ethereum: a secure decentralised generalised transaction ledger[J]. Ethereum Project Yellow Paper, 2014, 151: 1-32.

[17] JIANG B, CHEN Y F, WANG D, et al. WANA: symbolic execution of wasm bytecode for extensible smart contract vulnerability detection[C]//Proceedings of 2021 IEEE 21st International Conference on Software Quality, Reliability and Security. Piscataway: IEEE Press, 2021: 926-937.

[18] ARAUJO F. A maximum independent set approach for collusion detection in voting pools[J]. Journal of Parallel and Distributed Computing, 2011, 71(10): 1356-1366.

[19] PELEG B, SUDHÖLTER P. Introduction to the theory of cooperative games[M]. Berlin: Springer Science & Business Media, 2007.

[20] LUCAS WF, BRAMS S J, LUCAS W F, et al. Measuring power in weighted voting systems[M]. Berlin: Springer, 1983.

[21] YANG X L, CHEN Y, CHEN X H. Effective scheme against 51% attack on proof-of-work blockchain with history weighted information[C]//Proceedings of 2019 IEEE International Conference on Blockchain (Blockchain). Piscataway: IEEE Press, 2019: 261-265.

[22] ALMALLOHI I A I, ALOTAIBI A S M, ALGHAFEES R, et al. Multivariable based checkpoints to mitigate the long range attack in proof-of-stake based blockchains[C]//Proceedings of the 3rd International Conference on High Performance Compilation, Computing and Communications. New York: ACM Press, 2019: 118-122.

[23] WANG L, ZHU Q H, LI B Z. Extensive game analysis and improvement strategy of DPOS consensus mechanism[J]. The Journal of China Universities of Posts and Telecommunications, 2021(5): 27-35, 101.

[24] 田国华, 胡云瀚, 陈晓峰. 区块链系统攻击与防御技术研究进展[J]. 软件学报, 2021, 32(5): 1495-1525.
TIAN G H, HU Y H, CHEN X F. Research progress on attack and defense techniques in block-chain system[J]. Journal of Software, 2021, 32(5): 1495-1525.

[25] 魏松杰, 吕伟龙, 李莎莎. 区块链公链应用的典型安全问题综述[J]. 软件学报, 2022, 33(1): 324-355.
WEI S J, LÜ W L, LI S S. Overview on typical security problems in public blockchain applications[J]. Journal of Software, 2022, 33(1): 324-355.

[26] LUO Y H, CHEN Y Q, CHEN Q, et al. A new election algorithm for DPos consensus mechanism in blockchain[C]//Proceedings of 2018 7th International Conference on Digital Home (ICDH). Piscataway: IEEE Press, 2018: 116-120.

[27] YAO Y J, TIAN F, ZHANG C. The research of an improved blockchain consensus mechanism[C]//Proceedings of 2020 2nd International Conference on Applied Machine Learning (ICAML). Piscataway: IEEE Press, 2020: 305-310.

[28] WANG L J, XU P H, SU W, et al. Research on improvement of blockchain DPOS consensus mechanism based on HK clustering[C]//Proceedings of 2021 China Automation Congress (CAC). Piscataway: IEEE Press, 2021: 1167-1172.

[29] AZIZ H, BACHRACH Y, ELKIND E, et al. False-name manipulations in weighted voting games[J]. Journal of Artificial Intelligence Research, 2011, 40: 57-93.

[30] HART S. Game theory[M]. London: Palgrave Macmillan, 1989.

[31] BANZHAF III, JOHN F. Weighted voting doesn’t work: a mathematical analysis[J]. Rutgers Law Review, 1965, 19: 317-343.

[32] SAAD W, HAN Z, DEBBAH M, et al. Coalitional game theory for communication networks[J]. IEEE Signal Processing Magazine, 2009, 26(5): 77-97.

[33] KUMAR P, KUMAR A A, SAHAYAKINGSLY C, et al. Analysis of intrusion detection in cyber attacks using DEEP learning neural networks[J]. Peer-to-Peer Networking and Applications, 2021, 14(4): 2565-2584.

[34] TURNOVEC F. Trends in multicriteria decision making[M]. Berlin: Springer, 1998.
[35] CHEN W L, GUO X F, CHEN Z G, et al. Phishing scam detection on ethereum: towards financial security for blockchain ecosystem[C]//Proceedings of the Twenty-Ninth International Joint Conference on Artificial Intelligence. California: International Joint Conferences on Artificial Intelligence Organization, 2020: 4506-4512.
[36] LIN D, WU J J, YUAN Q, et al. Modeling and understanding ethereum transaction records via a complex network approach[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2020, 67(11): 2737-2741.
[37] WEI Y X, LIANG L, ZHOU B, et al. A modified blockchain DPoS consensus algorithm based on anomaly detection and reward-punishment[C]//Proceedings of 2021 13th International Conference on Communication Software and Networks (ICCSN). Piscataway: IEEE Press, 2021: 283-288.

[作者简介]

付晓东（1975− ），男，云南镇雄人，博士，昆明理工大学教授，主要研究方向为服务计算、智能决策、可信计算等。

漆鑫鑫（1998− ），男，湖北黄石人，昆明理工大学硕士生，主要研究方向为服务计算、区块链等。

刘骊（1979− ），女，重庆人，博士，昆明理工大学教授，主要研究方向为服务计算、计算机视觉、视频图像处理等。

彭玮（1980− ），女，湖南娄底人，博士，昆明理工大学教授，主要研究方向为生物信息学、数据挖掘、机器学习等。

丁家满（1974− ），男，江西于都人，博士，昆明理工大学教授，主要研究方向为数据挖掘、云计算、软件工程等。

代飞（1982− ），男，四川乐山人，博士，西南林业大学教授，主要研究方向为服务计算、人工智能、软件工程等。