Collusion Attack Analysis and Detection of DPoS Consensus Mechanism

Xinxin Qi[1], Xiaodong Fu[1,2](✉), Fei Dai[3], Li Liu[1,2], Lijun Liu[1,2], Jiaman Ding[1,2], and Wei Peng[1,2]

[1] Yunnan Provincial Key Laboratory of Computer Technology Application, Kunming 650500, China
xiaodong_fu@hotmail.com
[2] Faculty of Information Engineering and Automation, Kunming University of Science and Technology, Kunming 650500, China
[3] College of Big Data and Intelligent Engineering, South Forestry University, Kunming 650224, China

Abstract. With the development of blockchain technology, the increasing safety accidents result in huge economic losses in blockchain systems. Delegated Proof of Stake (DPoS) selects the witness nodes to produce blocks by voting, leading to the quick confirmation of transactions. As one of the widely used consensus mechanisms in public blockchain, DPoS is still threatened by attacks. In this paper, an analysis method for collusion attacks of DPoS consensus mechanism is proposed. Meanwhile, we analyze the behavioral motivations of malicious nodes and detect the attacks that exist in the voting process of DPoS. First, the coalitional game is the basic form of cooperative game, which can be used to analyze the structure, strategy and benefits of cooperative game. We build a coalitional game model to analyze motivations of DPoS nodes that launched collusion attacks. And then we use the Shapley-Shubik power index and Banzhaf power index in weighted voting games of DPoS, which calculated different values that DPoS suffered attacks during the voting phase. Experimental results show that collusion attacks in DPoS can be effectively detected by this method. In addition, the analysis results can further contribute to the security of the DPoS blockchain system.

Keywords: Blockchain · Consensus mechanism · DPoS · Collusion attack · Coalitional game · Weighted voting game

1 Introduction

Bitcoin is a cryptocurrency proposed by Satoshi Nakamoto in 2008 in the form of peer-to-peer (P2P) [1]. Since then, people gradually pay more attention to blockchain technology used in Bitcoin. Blockchain is widely used in finance, the Internet of Things, transportation and other fields because of its characteristics of decentralization, non-tamper ability, collective maintenance, etc. Generally speaking, the consensus mechanism, as an important part of the blockchain, undertakes the consistency and security of blockchain's data. The performance of the consensus mechanism directly affects the security, transaction

D. Svetinovic et al. (Eds.): BlockSys 2022, CCIS 1679, pp. 194–206, 2022.
https://doi.org/10.1007/978-981-19-8043-5_14

processing capabilities, and scalability of blockchain systems. However, due to the complexity of the blockchain technology structure and the lack of security control, attacks on blockchain systems are increasing rapidly. For example, on January 5–8, 2019, due to the decline in ETC's market capitalization and subsequent decline in network computing power, malicious attackers used network computing power to carry out at least 15 suspected double-spend attacks on the ETC blockchain. This resulted in 219,500 ETC attacks, or about $1.1 million. However, the cost of this attack was only about $20,000, and the malicious attacker benefited 50 times.

Currently, there are several common consensus mechanisms in blockchain. Among them**,** Proof-of-Work (PoW) is the consensus mechanism used in Bitcoin system. Principle of PoW is that nodes compete through computing power to decide who can produce blocks and get rewards. This process is also called mining. Although this process is simple and easy to achieve, the process of achieving consensus through "mining" creates waste of resources. In order to solve the problem of resource wasting in PoS [2], Sunny King, the founder of Peercoin, proposed proof of stake (PoS) in the white paper. And PoS is attracted widespread attention as soon as it was proposed. PoS avoids the waste of resources, but the process of reaching consensus is easy to produce monopolies. There are also various risks of being attacked in PoS. Subsequently, in April 2014, Dan Larimer (BM), the lead developer of Bitshares, proposed the Delegated proof of stake (DPoS) [3]. DPoS is now used on platforms such as Ethereum, EOS, etc.

In DPoS consensus mechanism, each node has voting rights. Then, some delegates, or super-nodes are elected based on the vote. These super-nodes have complete equal rights to each other. In the end, they take turns producing blocks. If delegates fail to perform their duties (such as failing to generate blocks when it's their turn), they are removed and the network chooses new super-nodes to replace them. Although, in the process, nodes reach consensus very quickly, in other words, nodes produce blocks quickly, the process still creates some problems. For example, whether there is bad behavior or whether there are various attacks in voting between nodes. That is, whether there are malicious nodes manipulating the results of voting. This also raises the question of how to measure the power of different participants in a cooperative environment. Because, in voting games, the player's weight does not fully reflect the player's actual power over an alliance decision. The power here can be understood as the prior probability that the player will play a key role in the game. The power index [4] is a measure of a player's ability to influence the outcome of a game in the context of a weighted voting game. Two most common power indices are Shapley-Shubik power index and Banzhaf power index.

In order to effectively analyze and detect collusion attacks in DPoS, this paper uses cooperative game theory as the theoretical basis [5], analyzes the malicious nodes conspiring with other nodes in election of DPoS. Meanwhile, we get comparative experimental data through the Shapley-Shubik power index and the Banzhaf power index. In order to show the effectiveness of this proposed method, we compare our method with the literature [6] by Pearson correlation coefficient. The results of experiment obtained by this method show that the attacker can increase his power in election through collusion, and manipulate the election results in the end. At the same time, detecting attacks is more effective than [6].

The contribution of this paper can be summarized as follows.

- We analyze the collusion attack in DPoS consensus mechanism by using game theory and Shapley-Shubik power index and Banzhaf power index, and the attacker's behavioral motivation can be effectively analyzed through experiments.
- We detect collusion attacks in DPoS through the coalitional game model and the magnitude of changes in two power indices. In order to highlight the superiority of our method, we compare with other experiments by using Pearson correlation coefficient.

The remainder of paper is organized as follows. Section 2 reviews related work. Section 3 introduces the related background knowledge. Section 4 shows the coalitional model of DPoS in game theory and definition of various methods and indicators. The experimental results are shown in Sect. 5. Section 6 concludes and discuss the future work.

2 Related Work

In order to alleviate the 51% attack in PoW, Yang et al. [7] proposed a scheme to combine history weighted information of miners with total calculation difficulty. And for long range attack in PoS, AlMallohi et al. [8] put forward to a new strategy for implementing checkpoints in blockchain technology, which could mitigate long range attacks. In the weighted voting game on DPoS, collusion attacks aim at forming a collusive coalition. They can select delegated nodes to participate in the final consensus phase of DPoS by this way. The delegated nodes selected by malicious attackers can interfere with the final consensus result, in consensus phase of DPoS. Finally, they benefit themselves by causing massive damage to the blockchain system. Up to now, some scholars have conducted relevant research on the above issues. We divide the types of research into two categories, one is theoretical and strategic analysis, the other is improvement of consensus mechanism.

1. Theoretical and strategic analysis. W. lei et al. [9] proposed a game analysis method on DPoS, which could well theoretically analyze to show that there are malicious attacks. In 2021, Tian and Hu [10] have compiled various attacks and defense methods against blockchain systems that are already known. Wei et al. [11] introduced blockchain technology, reviewing the security risks in blockchain. Secondly, the security issues in this paper are classified and summarized. Finally, they looked forward to the current research hotspots and development trends of blockchain security.
2. Improvement of consensus mechanism. Y. Luo et al. [12] in 2018 proposed a new election algorithm for the DPoS consensus mechanism to strengthen the characteristics of decentralization. Xu et al. [13] put forward a kind of vague set to improve DPoS. At the same time, this article improves the security and fairness of the blockchain. Y. Yao et al. [14] improved the security of the blockchain network by using the fish swarm algorithm during the voting stage of DPoS.

At present, there are endless attacks on the consensus process of DPoS. If we don't analyze these attacks, blockchain systems still face significant risks and even huge losses. What's more, given the peculiarities of DPoS consensus, scholars have not yet analyzed the attacks encountered during the node voting process in the original DPoS.

3 Preliminaries

3.1 DPoS: Delegated Proof of Stake

The consensus mechanism emerged, because of "Byzantine Generals Problem" in blockchain. In order to solve this problem, Miguel Castro and Barbara Liskov proposed the Byzantine fault-tolerant algorithm [15] in 1999. Currently, more common than other consensus mechanisms are proof of work (PoW), proof of stake (PoS), and delegate proof of stake (DPoS).

To better understand the principles of DPoS, we we consider the more common case of 21 delegate nodes. The voting nodes of DPoS participating in elections are defined as a finite set $N = \{n_1, n_2, n_3, \ldots\}$, and because the voting weight of DPoS nodes is proportional to their stake. Their stake or voting weight is defined as a finite set $W = \{w_1, w_2, w_3, \ldots\}$. During the voting phase of DPoS, the voting nodes N elect 21 delegate nodes according to voting weight W. These nodes take turns producing blocks for a given amount of time, and the remaining members validate and, eventually reach consensus. This is a visual description of the DPoS (Delegated Proof of Stake) consensus mechanism (Fig. 1).

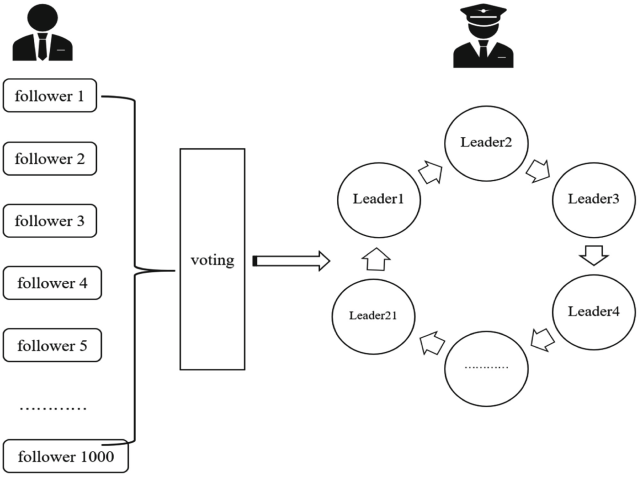

Fig. 1. The model of weighted voting in DPoS

3.2 Weighted Voting Games

Under the well-known majority voting, every voter has the same power. However, the power of all voters cannot be always equal. In parliamentary elections, each party has different seats, and when voting on whether a bill passes, each party has different power. Besides, in the process of consensus among the nodes of DPoS, the nodes vote according to their stake, and the stake of each node are different. This form of voting games called weighted voting games. During the voting process of DPoS, the nodes form different coalitions, and when a coalition meets or exceeds the prescribed quota, it becomes the winning coalition. The quota mentioned here is defined as q. A weighted voting game in DPoS is defined as $G = (N, W, q)$.

3.3 Collusion Attack

Collusion is a secret cooperation between two or more parities that restricts open competition by deceiving, misleading, or deceiving another person's legal right. In the study of economics, collusion occurs within the industry when companies cooperate for mutual benefit. For example, it was revealed that both companies agreed not to hire each other's employees to stop wage increases, in a 2015 case of collusion between Google and Apple for employee poaching.

During the voting process, malicious nodes collude with other nodes to form an alliance through various means to manipulate the election results. Usually, this kind of attack is called a collusion attack [16]. Such as, in 2018 Venezuelan presidential election, reports of vote purchases were common during the presidential campaign. Hungry Venezuelans were forced to vote for Maduro as the government bribed potential supporters with food. Consequently, collusion attack of DPoS in the weighted voting process need to be rationally analyzed and detected (Fig. 2).

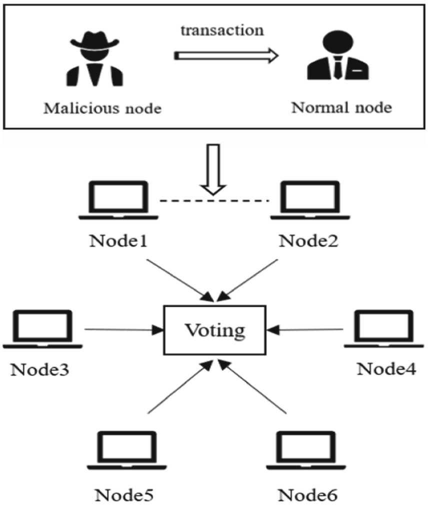

Fig. 2. The model of collusion attack

4 Model and Definitions

In order to analyze collusion attacks in DPoS, we use the coalitional game model and two power indices as analytical methods and tools. At the same time, we use the Pearson correlation coefficient as an indicator of the effectiveness and superiority of detecting attack. For defending against attacks, we also consider using saturation activation functions to constrain the behavioral motivations of the attack nodes. The above research models and methods are defined in the following definition.

4.1 Coalitional Games in DPoS

In a cooperative game, when agents form alliances for the same goal, we can model the system as a coalitional game. A coalitional game $C = (N, v)$, consist of [17]:

- a finite set $N = (1, 2, 3 \ldots n)$, of nodes participating in voting and
- a function $v : 2^N \rightarrow R$. In a simple coalitional game, we say v only takes values in $\{0, 1\}$. We say a coalition $S \subseteq P$ wins if $v(S) = 1$, otherwise loses.

The weighted voting game is a well-known model of cooperative game in the field of voting. At the same time, the weighted voting game in DPoS is a simple coalitional game that can be described as a non-negative weight vector W and a positive quota q. Moreover, when the weight of a coalition S meets and exceeds the quota (i.e., $\sum_{i \in S} w_i \geq q$), it will win (i.e., $v(S) = 1$). We can also use $G = (C, W, q) = (N, W, q, v)$ denotes the weighted voting game in DPoS.

Given a weighted voting game G in DPoS, a voting node $i \in S$ is pivotal in the winning coalition S, if S becomes a losing coalition after the voting node i leaves coalition S(i.e. $v(S) = 1$ and $v(S \backslash i) = 0$). Since the influence of individual voting node on the game is obvious and related to the indicator of measuring power, we need to make accurate calculations of the voting nodes in DPoS by using two power indices. The following two power indices are described in detail.

4.2 SSI: Shapley-Shubik Power Index

The Shapley value [18] reflects the average marginal contribution or expected marginal contribution of the participants. Usually, when it's applied to the voting games, the Shapley value of nodes is the Shapley-Shubik power index. Since elections in DPoS are also voting games, we can calculate the Shapley-Shubik power index of voting nodes. The Shapley-Shubik power index is given by $SSI(G) = SSI(N, W, q, v) = (SSI_1(N, W, q, v), SSI_2(N, W, q, v), \ldots, SSI_n(N, W, q, v))$ where the Shapley-Shubik power index of node i:

$$v(S) = \begin{cases} 1 \sum\limits_{i \in S} w_i \geq q \\ 0 \; otherwise \end{cases} \tag{1}$$

$$SSI_i(N, v) = \sum_{S \subseteq N | i \in S} \tfrac{(|S|-1)!(n-|S|)!}{n!} [v(S) - v(S \backslash \{i\})] \tag{2}$$

The formula calculates the contribution of node i to all coalitions and adds them up. $\frac{(|S|-1)!(n-|S|)!}{n!}$ represents the probability that node i joined the coalition $S - \{i\}$. Its denominator represents the number of permutations of n nodes, and the numerator represents the number of permutations with the coalition $S - \{i\}$, then node i enters the coalition $S - \{i\}$, and finally multiplied by the number of permutations with the others. $[v(S) - v(S \backslash \{i\})]$ is the value that node i contributed to the coalition S.

4.3 PBI: Banzhaf Power Index or Penrose Index

The Banzhaf power index [19], refers to the power of a voter in the fact that he(she) can make a winner by joining a coalition that supposed to lose, which also means he can make it lose by turning his back on a coalition that meant to be won. That said, he is a "key joiner" to the coalition. In this paper, we deem that the voting nodes' Banzhaf power index is the number of winning coalitions when it is a "key joiner". The Banzhaf power index is given by $PBI(G) = PBI(N, W, q, v) = (PBI_1(N, W, q, v), PBI_2(N, W, q, v), \ldots, PBI_n(N, W, q, v))$ where the Banzhaf power index of node i:

$$PBI_i(N, v) = \frac{1}{2^{n-1}} \sum_{S \subseteq N | i \in S} [v(S) - v(S \backslash \{i\})] \tag{3}$$

4.4 The Weighted Voting Game in DPoS

Detection of Collusion Attacks in DPoS. Since, the nodes of weighted voting game in DPoS select n delegate nodes participating in the production of blocks according to the majority criterion, given a set of weighted voting game $\overline{G} = [G_1, G_2, \ldots, G_k, \ldots]$. Based on the Banzhaf power index and Shapley-Shubik power index, we can analyze the difference of two power indices before and after collusion attack in DPoS. We can judge whether there was a collusion attack, based on the magnitude of the change in the minimal power index before and after the formation of coalition in the n weighted voting sets.

Let M_k be a magnitude of the change in the k-th voting partition. Let $\widetilde{SSI}(G_k)$ and $\widetilde{PBI}(G_k)$ be the smallest Shapley-Shubik and Banzhaf power index after the formation of the coalition. Let $\overset{\backsim}{SSI}(\ G_k)$and $\overset{\backsim}{PBI}(\ G_k)$be the smallest power indices before the formation of the coalition. Then we write:

$$M_k \ = \frac{1}{2}\left(\frac{\widetilde{SSI}(\ G_k)}{\overset{\backsim}{SSI}(\ G_k)} + \frac{\widetilde{PBI}(\ G_k)}{\overset{\backsim}{PBI}(\ G_k)}\right) \tag{4}$$

For a more rational analysis, we classify the types of attackers in the attack, let M_k^l and M_k^h is the lowest and highest magnitude of variation in collusion attacks. At the same time, let $D_k(M_k)$ denote the result of whether there is an attack on the k-th weighted voting game partition in $\overline{G}$. That is to say,

$$D_k(M_k) = \begin{cases} 1 & M_k^l \leq M_k \leq M_k^h \, for\ every\ G_k \in \overline{G} \\ 0 & otherwise \end{cases} \tag{5}$$

To demonstrate the effectiveness of the method, we refer to Pearson correlation coefficient. Let A is a set of m-dimensional vectors that set the number of collusion attacks. Let $\overline{A}$ is average of A-vector elements. Let D be a set of calculated m-dimensional vectors, let $\overline{D}$ is average of D-vector elements, where:

$$\begin{cases} D = \left(D_1, D_2, \ldots D_j, \ldots D_m\right) \\ D_j = \sum_{i=1}^{n} D_k(M_k\ ) \end{cases} \tag{6}$$

According to the definition of Pearson correlation coefficient, the following formula can be obtained:

$$Pcc(A, D) = \frac{\sum_{j=1}^{m}\left(\left(A_j - \overline{A}\right) \times \left(D_j - \overline{D}\right)\right)}{\sqrt{\sum_{j=1}^{m}\left(\left(A_j - \overline{A}\right)\right)^2} \times \sqrt{\sum_{j=1}^{m}\left(\left(D_j - \overline{D}\right)\right)^2}} \tag{7}$$

5 Experiment and Analysis

In order to analyze the collusion attack on the weighted voting process among nodes in DPoS, this paper performs simulation experiments from the public X-Block dataset. The dataset contains tagged privacy data as well as transaction data for some Ethereum blockchain nodes. At the same time, all experiments were conducted on a PC with Intel Core i7-11700k 3.6 GHz CPU and 16 GB RAM. The programs are implemented in PyCharm 2021.3. In our next work, we use Shapley-Shubik and Banzhaf power index to analyze collusion attackers in DPoS. And, we highlight the effectiveness of the power index-based detection through the Pearson correlation coefficient.

5.1 Analysis of Collusion Attack in DPoS

To be able to simulate a simple and realistic DPoS voting process, we ony consider the situation when $k = 21$. That is, we set up 21 weighted voting games in DPoS. According to the particularity of weighted voting in DPoS. The tagged privacy data of Ethereum nodes is divided into 21 weighted voting games. And the 21 partitions simulate the difficulty of selecting the 21 delegate nodes with the most votes in the DPoS blockchain in the order of increasing total weights. In order to get effective analysis results, we selected attackers with the same weight in 21 weighted voting game, and divide the attackers who participate in the weighted vote into two types with larger weights and smaller weights, and conducted experiments separately.

First, according to the above model and definition, we need to experiment with the values of two power indices before and after the collusion attack of malicious nodes in DPoS. The experimental results are divided into Fig. 3 and Fig. 4. The black and red lines in Fig. 3 and Fig. 4 represent the magnitude of changes in two power indices of the attacker before and after the launch of collusion attack, respectively.

We then use the squares to represent the specific values of the attacker's power index before and after the collusion attack when the attacker has a larger weight. For the case when the attacker has a small weight, we use a diamond shape to represent the specific value of the attacker.

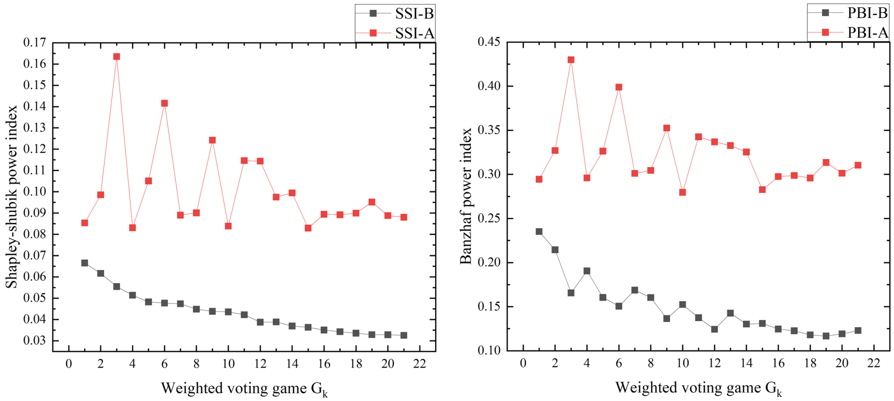

Fig. 3. Two power indices values before and after the collusion attack, when the attacker has a larger weight

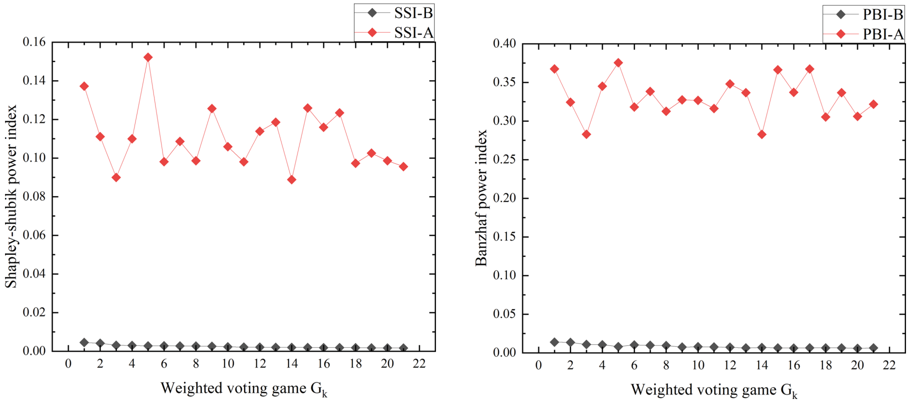

Fig. 4. Two power indices values before and after the collusion attack, when the attacker has a lower weight

Based on the above results (Fig. 3 and 4), regardless of the type of malicious node that launched the collusion attack, its two power indices will increase. That is to say, the attackers will be motivated to launch this attack by increasing their power in weighted voting game.

Furthermore, Fig. 3 is more pronounced than Fig. 4, proving that the Shapley-Shubik power index is monotonic [20] before the launch of collusion attack. In other words, it's cheaper for an attacker to manipulate a lower-ranked election through the collusion attack than a top-ranked election. For the Banzhaf power index, Fig. 3 also shows more clearly than Fig. 4 that there is no regular change in the value of PBI of the same weight in different weighted votes.

All in all, these two power indices can help us analyze the attacker's motives for evil from the individual rationality of game theory. And we can use this as an entry point to further look for collusion attacks in different weighted voting games.

5.2 Detection of Collusion Attack in DPoS

In order to show the effectiveness and superiority of the detection method of this paper, we divide the comparative experiment into two categories: self-comparison and method comparison.

Muti-group Detection. Let's first assume that the vector containing the voting partition where there is a collusion attack. Since, in DPoS, 21 delegate nodes are selected, then let a five-dimensional vector (3, 6, 9, 12, 16) represents the number of partitions with the attack.

Figure 5 visually shows the comparison of setpoints and analytical values. The horizontal axis representing the elemental ordinal number of the vector and the vertical axis representing the number of partitions which contain the attack in the weighted voting game G_i. Although, it is shown that the detection value is not much different from the set value, we still need to compare with more specific metrics.

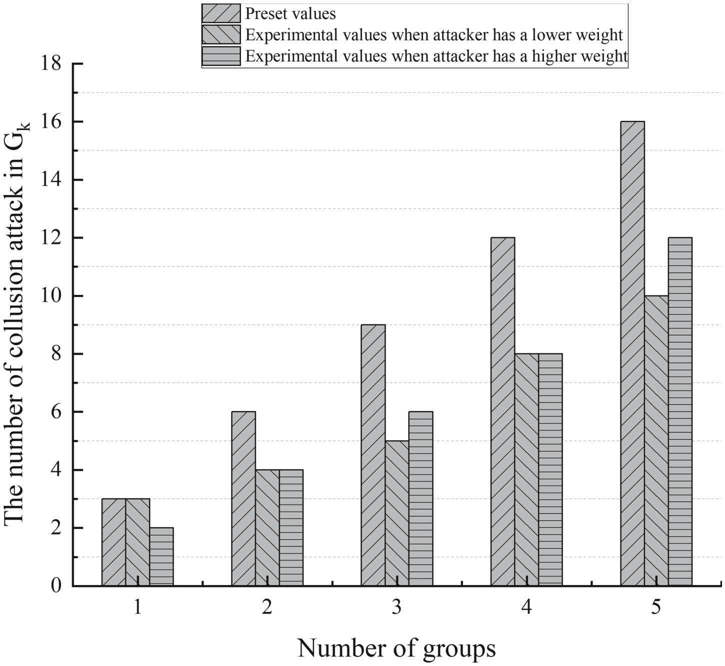

Fig. 5. The results of collusion attack analysis compared with the set value.

Comparison of Detection Effects. Similarity algorithms are often used in recommended environments. In this way, we can calculate the similarity between users by using the preferences of individual or all users for the whole items as vector. In this article, we measure the quality of the analysis method by the similarity between the set-point and the detected value. Since the Pearson correlation coefficient is more reflective in trend of movement between vectors than Euclidean distance, And it can compensate for the lack of dimensions compared to Cosine similarity. Besides, it can be used here to judge the effectiveness of the detection method. To highlight the effectiveness of this method, we compare this article with an anomaly detection algorithm mentioned in literature. The experimental data of literature will be obtained through the historical transaction data of some Ethereum blockchain nodes.

First of all, based on the nature of Pearson's correlation coefficient, we can know that the closer the value is to 1, the more positively correlated the two vectors are. The horizontal axis of Fig. 6 represents the dimensions of the vector and the vertical axis represents the Pearson correlation coefficient. That's to say, we analyze it by different experimental dimensions. Furthermore, we define the detection method in this article as PI, and the detection method of supporting vector machines in the literature as OSVM.

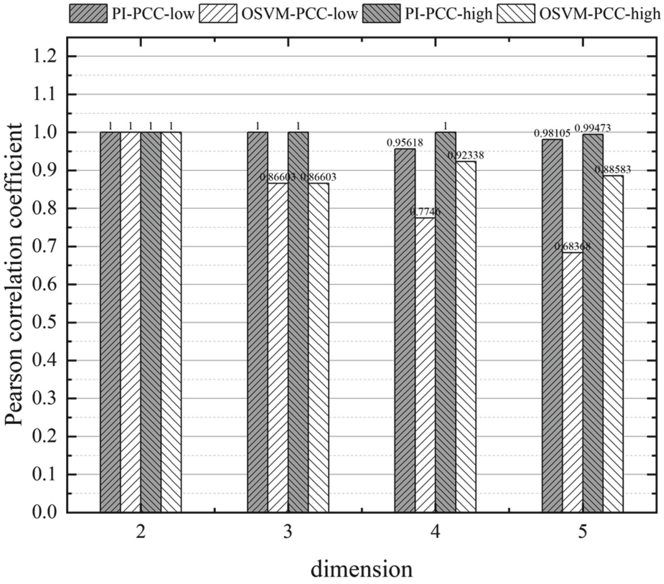

Fig. 6. The values of Pearson correlation coefficient with different dimension.

According to the results of Fig. 6, it is accurate to analyze the results of the attack by using the power indices, regardless of the type of attacker initiated the collusion attack. Furthermore, with the increase of dimensions, the method of this paper is better than the anomaly detection algorithm which is based support vector machine.

6 Conclusion

IN this paper, we presented an analysis method, which can detect the collusion attack in DPoS. We use the Shapley-Shubik power index and Banzhaf power index to analyze the motives for the attackers. At the same time, two power indices are used to effectively detect collusion attacks in DPoS. In order to highlight the superiority of the proposed method, we demonstrate the detection effect by Pearson correlation coefficient.

Although, we effectively analyze and detect collusion attacks in DPoS, how to prevent such attack is still a problem that needs to be solved. What's more, in order to ensure the security of blockchain systems, we still urgently need to establish effective and general prevention models for different consensus mechanisms. And in the next step, we can also consider whether we can apply this method to other similar consensus mechanisms to analyze whether similar attacks with the collusion attack exist. Then we can test the effectiveness of this method.

Acknowledgement. This work was partially supported by the National Natural Science Foundation of China (Grand No. 61962030, 61862036), the Yunnan Provincial Foundation for Leaders of Disciplines in Science and Technology (201905C160046). The Dou Wanchun Expert Workstation of Yunnan Province (202105AF150013).

References

1. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system (2008). https://bitcoin.org/bitcoin.pdf
2. Ometov, A., et al.: An overview on blockchain for smartphones: state-of-the-art, consensus, implementation challenges and future trends. IEEE Access **8**, 103994–104015 (2020). https://doi.org/10.1109/ACCESS.2020.2998951
3. Larimer, D.: Delegated proof-of-stake white paper (2014). http://www.bts.hk/dpos-baipishu.html
4. Lucas, W.F.: Measuring power in weighted voting systems. In: Brams, S.J., Lucas, W.F., Straffin, P.D. (eds.) Political and Related Models, pp. 183–238. Springer, New York (1983). https://doi.org/10.1007/978-1-4612-5430-0_9
5. Peleg, B., Sudhölter, P.: Introduction to the Theory of Cooperative Games. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-72945-7
6. Wei, Y., Liang, L., Zhou, B., Feng, X.: A modified blockchain DPoS consensus algorithm based on anomaly detection and reward-punishment. In: 2021 13th International Conference on Communication Software and Networks (ICCSN), Chongqing, China, pp. 283–288. IEEE (2021)
7. Yang, X., Chen, Y., Chen, X.: Effective scheme against 51% attack on proof-of-work blockchain with history weighted information. In: 2019 IEEE International Conference on Blockchain (Blockchain), pp. 261–265 (2019). https://doi.org/10.1109/Blockchain.2019.00041
8. AlMallohi, I.A.I., Alotaibi, A.S.M., Alghafees, R., Azam, F., Khan, Z.S.: Multivariable based checkpoints to mitigate the long range attack in proof-of-stake based blockchains. In: Proceedings of the 3rd International Conference on High Performance Compilation, Computing and Communications, pp. 118–122. Association for Computing Machinery, New York (2019). https://doi.org/10.1145/3318265.3318289
9. Lei, W., Qinghua, Z., Baozhen, L.: Extensive game analysis and improvement strategy of DPOS consensus mechanism. J. China Univ. Posts Telecommun. **28**, 27–35 (2021). https://doi.org/10.19682/j.cnki.1005-8885.2021.0030
10. Guo-Hua, T., Yun-Han, H.U., Xiao-Feng, C.: Research progress on attack and defense techniques in block-chain system. J. Softw. **32**, 1495–1525 (2021)

11. Song-Jie, W.E.I., Wei-Long, L., Sha-Sha, L.I.: Overview on typical security problems in public blockchain applications. J. Softw. **33**, 324–355 (2021)
12. Luo, Y., Chen, Y., Chen, Q., Liang, Q.: A new election algorithm for DPos consensus mechanism in blockchain. In: 2018 7th International Conference on Digital Home (ICDH), Guilin, China, pp. 116–120. IEEE (2018)
13. Xu, G., Liu, Y., Khan, P.W.: Improvement of the DPoS consensus mechanism in blockchain based on vague sets. IEEE Trans. Ind. Inf. **16**, 4252–4259 (2020)
14. Yao, Y., Tian, F., Zhang, C.: The research of an improved blockchain consensus mechanism. In: 2020 2nd International Conference on Applied Machine Learning (ICAML), pp. 305–310 (2020). https://doi.org/10.1109/ICAML51583.2020.00069
15. Wang, H., Guo, K.: Byzantine fault tolerant algorithm based on vote. In: 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), pp. 190–196 (2019). https://doi.org/10.1109/CyberC.2019.00041
16. Araujo, F., Farinha, J., Domingues, P., Silaghi, G.C., Kondo, D.: A maximum independent set approach for collusion detection in voting pools. J. Parallel Distrib. Comput. **71**, 1356–1366 (2011). https://doi.org/10.1016/j.jpdc.2011.06.004
17. Saad, W., Han, Z., Debbah, M., Hjorungnes, A., Basar, T.: Coalitional game theory for communication networks. IEEE Sig. Process. Mag. **26**, 77–97 (2009)
18. Hart, S.: Shapley value. In: Eatwell, J., Milgate, M., Newman, P. (eds.) Game Theory, London, UK, pp. 210–216. Palgrave Macmillan (1989). https://doi.org/10.1007/978-1-349-20181-5_25
19. Banzhaf, J.F.I.: Weighted voting doesn't work: a mathematical analysis. Rutgers Law Rev. **19**, 317 (1964)
20. Turnovec, F.: Monotonicity of power indices. In: Stewart, T.J., van den Honert, R.C. (eds.) Trends in Multicriteria Decision Making, pp. 199–214. Springer Berlin Heidelberg, Berlin, Heidelberg (1998). https://doi.org/10.1007/978-3-642-45772-2_17