Characterizing Coin-Based Voting Governance in DPoS Blockchains

Chao Li[1], Runhua Xu[2], Li Duan[1]

[1]School of Computer and Information Technology, Beijing Jiaotong University, China
[2]School of Computer Science and Engineering, Beihang University, China
{li.chao, duanli}@bjtu.edu.cn, runhua@buaa.edu.cn

Abstract

Delegated-Proof-of-Stake (DPoS) blockchains are governed by a committee of dozens of members elected via coin-based voting mechanisms. This paper presents a large-scale empirical study of two critical characteristics, personal impact and participation rate, of three leading DPoS blockchains. Our findings reveal the existence of decisive voters whose votes can alter election outcomes, as well as the fact that almost half of the coins have never been used in committee elections. Our research contributes to demystifying the actual use of coin-based voting governance and offers novel insights into the potential security risks of DPoS blockchains.

Introduction

With the fast development of blockchain technologies, it has become a trend to build various types of applications, ranging from social media platforms to games, in a decentralized manner. In blockchains, it is necessary to rely on consensus protocols to provide data consistency among nodes in a peer-to-peer network. As the most well-known consensus protocol, the Proof-of-Work (PoW) consensus protocol has secured Bitcoin (Nakamoto 2008) and Ethereum (Wood 2014) for almost a decade. However, PoW requires decentralized consensus to be fulfilled in a large-scale peer-to-peer network (Lin et al. 2021). The lengthy time necessary to gain consensus results in very low transaction throughput, making it impossible for PoW to meet the practical requirements of a variety of applications (Croman et al. 2016).

To overcome the throughput issue, the Delegated Proof-of-Stake (DPoS) consensus protocol (Larimer 2014) has become increasingly popular in recent years and has supported various successful projects, such as EOSIO (He et al. 2021), Steem (Guidi 2020) and TRON. In DPoS blockchains, both the production of blocks and the governance of blockchains are managed by a committee of dozens of members who are periodically elected by holders of coins (i.e., cryptocurrencies) via coin-based voting mechanisms. Specifically, coin holders need to first freeze their coins to acquire a proportional amount of voting power, and then cast voting-power-weighted votes to elect a number of candidates (e.g., 21 in EOSIO) to form a committee. The committee has two primary responsibilities. First, each committee member produces a block in turn. Second, the committee is in charge of decision-making, including updating global settings, blocking specific users, and even overturning historical transaction results that have been confirmed. The extensive authority of the committee may be advantageous from the point of view of efficiency, but may bring hidden dangers from the point of view of security. For instance, a wealthy coin holder might convert a decentralized network into one susceptible to centralized authority by controlling the supermajority of committee members through voting-power-weighted votes. Even if no voter has a significant impact on the election, the addition of coins that have not previously participated in the election may alter the outcome. However, little is known about the personal impact (i.e., wealthy coin holders) and participation rate (i.e., the proportion of frozen coins) of committee elections in DPoS blockchains.

In this paper, we present a large-scale empirical study of these two critical characteristics, personal impact and participation rate, of three leading DPoS blockchains, namely EOSIO, Steem and TRON. Based on data collected from the three blockchains, we analyzed and recreated daily snapshots of the committee elections for the three blockchains during the two-year period from August 2018 to July 2020. Our findings indicate that between August 2018 and February 2020, a single voter can influence up to twenty percent of committee seats in any of the three blockchains. However, during TRON's takeover of Steem in Match 2020, we observed that nearly the whole Steem committee was dominated for months by a single voter. Our results also show that, in EOSIO, Steem and TRON, only about half of the coins have been actually used in committee elections. The remaining coins are not frozen and are not used in elections, allowing adversaries to use them to take over DPoS blockchains. We observed a surge in the participation rate in Steem in March 2020, which suggests that attacks using unfrozen coins are a serious threat that has already occurred. Our research in this paper characterizes coin-based voting governance and helps people from a variety of areas gain a grasp of the theory and actual use of coin-based voting governance in DPoS blockchains. In addition, our research offers novel insights into the potential security risks of DPoS blockchains and facilitates further research on the security of DPoS blockchains.

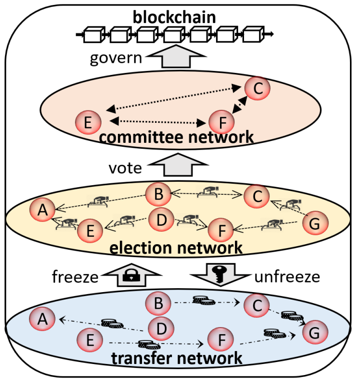

Figure 1: A layered abstract model for DPoS Blockchains

DPoS Blockchains

In this section, we first present a layered abstract model for DPoS blockchains and then depict the three core phases of coin-based voting governance. Finally, we introduce the background of three leading DPoS blockchains.

Layered Abstract Model

The leading DPoS blockchains, such as EOSIO, Steem, and TRON, have millions of users and permit a wide variety of operations. Among the various types of operations, the three most essential ones are *transfer*, *vote* and *govern*, which correspond to the three networks depicted in a layered abstract model in Fig. 1.

Transfer network. The *transfer* operation allows users to transfer their coins to other users, forming a transfer network. For instance, in Fig. 1, both user C and user F transferred some coins to user G. The coins in the transfer network are liquid and not frozen.

Election network. Users can cast their votes to up to X candidates through the *vote* operation, which forms an election network. In Fig. 1, we can see that user D voted for user E, while user E voted for user A. Most DPoS blockchains, such as EOSIO, Steem and TRON, set X to 30.

Committee network. Finally, DPoS blockchains enable committee members to execute a number of specialized governance operations. The committee members form a small network, and consensus regarding blockchain governance is only required within this network. In Fig. 1, among the users A to G, only three users, namely C, E and F, were elected as committee members.

Coin-based Voting Governance

The aforementioned three networks are connected to form a layered abstraction model through the following three core phases of coin-based voting governance, which gradually transforms users' coins into voting power and, finally, governance power.

Freezing. In the first phase, users need to freeze the liquidity of their coins in order to gain voting power. It is the voting power, not the coin itself, that gives a user's votes weight. This design embodies the core idea of Proof of Stake, which is incentive compatibility. Concretely, in DPoS blockchains, incentive compatibility makes rational users inclined to vote for candidates they believe will benefit the collective interests of that blockchain community. As shown in Fig. 1, the freeze on coin liquidity can grant users access to the election network from the transfer network.

Voting. In the second phase, users who have entered the election network become voters and then need to choose a voting strategy. Typically, a voter's voting strategy consists of three interrelated components: how many votes to cast, whom to vote for, and how much voting power to assign to each vote. At the end of each election cycle, the system ranks all candidates based on the voting power they have received, and the top Y candidates form a new committee in charge of governing the blockchain network until the next election cycle arrives.

Governing. In the third phase, the top Y candidates become committee members and then need to both maintain and govern the blockchain network. The main task of committees is to process proposals. Proposals can be used to adjust a variety of network parameters (e.g., account creation fee), enable or disable specific functionality (e.g., account renaming), and even modify users' private keys and reverse confirmed transactions. For example, in 2018, an EOSIO user had his account's private key stolen and reached out to the EOSIO community for assistance. EOSIO subsequently approved the very first proposal to alter private keys.

Leading DPoS Blockchains

We introduce the background of EOSIO, Steem and TRON.

EOSIO. EOSIO aims to build a general blockchain platform to serve various decentralized applications, like Windows on PC and Android on cell phones. Its goal is to enable more developers to quickly and easily build decentralized applications based on its platform, network and tools. Meanwhile, EOSIO is gradually building its own marketplace and ecosystem by issuing coins. EOSIO consistently ranks among the top 10 blockchain projects in the world.

The implementation of coin-based voting governance in EOSIO is as follows: (1) each user can vote for up to 30 candidates for committee election; (2) the top 21 candidates form a committee and govern the network until the next election; (3) any proposal requiring execution must receive at least 15 approvals from committee members.

Steem. Steem is designed to be a blockchain that supports various social applications. There are already over 300 decentralized applications based on Steem. Most of these applications are designed to serve social users. The most popular of these applications is *Steemit* (Li and Palanisamy 2019), a decentralized version of Reddit. In *Steemit*, users can create and share content as blog posts. Blog posts receive replies, reposts, upvotes or downvotes from other users and are ranked based on upvotes and downvotes. The blockchain creates a block every three seconds and periodically allocates coins to reward top-ranked posts.

Steem supports more than a million social users and has logged about a billion transactions. Steem encourages users to cast up to 30 voting-power-weighted votes for committee elections based on its coin-based voting governance. The top 21 candidates then become members of the committee. In

Steem, a proposal must receive at least 17 approvals from the 21 committee members to be adopted.

TRON. TRON is one of the youngest DPoS blockchains and is also one of the top 10 blockchains in the world. Similar to EOSIO, TRON supports smart contracts and, thus, various types of decentralized applications ranging from games to exchanges. TRON's financial ecosystem is very active and includes numerous cutting-edge decentralized financial applications, such as decentralized exchanges, non-fungible tokens and stable coins.

In TRON, a user can cast at most 30 votes and must split and assign her voting power across her votes. In addition, the committee consists of 27 members, and a proposal must receive at least 19 approvals in order to be approved.

Data Collection

In this section, we describe our data collection methodology. The Steem blockchain provides developers and researchers with an Interactive Application Programming Interface (API) for collecting and parsing blockchain data (Li et al. 2021). We collected raw data for 45,568,376 Steem blocks generated before July 2020. Similarly, from an API offered by TRON, we collected raw data for 21,980,572 TRON blocks generated between June 2018 and July 2020. For EOSIO, we utilized the dataset from a recent publication (Zheng et al. 2021), which contains 134,193,882 EOSIO blocks created prior to July 2020. Using the three datasets, we chose a two-year period, namely August 2018 to July 2020, to present the following empirical study.

Personal Impact in Governance

Personal impact in coin-based voting governance represents a critical dimension in understanding the security of DPoS blockchains. Imagine a single user has a considerable influence on committee elections. In that case, the blockchain might become a centralized system, with its decentralized nature existing only in name. We may conceive of an extreme instance. In the i^{th} election cycle, the EOSIO committee includes candidates No. 1 to 21. In the meantime, a wealthy voter appears and votes for candidates No. 31 to 51. Then, in the $(i+1)^{th}$ election cycle, all the original committee members, namely candidates No. 1 to 21, are replaced by candidates No. 31 to 51. In this way, the wealthy voter can indirectly control the blockchain network through candidates No. 31 to 51 and adopt any proposal, such as blocking certain users and reversing confirmed transactions.

This security risk does not merely exist in theory. In fact, incidents of this type have occurred recently. In March 2020, TRON took over the Steem blockchain within an hour and compelled the original Steem committee members to relinquish control of the Steem blockchain.

Next, we present the metric, methodology, results and insights of the empirical study of the personal impact in coin-based voting governance in EOSIO, Steem and TRON.

Metric and methodology. To measure the greatest personal impact on coin-based voting governance, we propose a metric named *personal impact index* (*PII*). In this paper, we define a single voter's impact as the difference between the election outcomes with and without the voter's votes. For instance, for ease of explanation, let's restrict the size of a committee to four, which makes the election outcome includes only four candidates. Then, during a specific election cycle, the election outcome includes candidates $\{A, B, C, D\}$. Next, for the same election cycle, we remove the votes cast by a certain voter from calculating the election outcome, retain votes cast by all the other voters and recompute the election outcome. Suppose the election outcome becomes $\{A, B, C, H\}$. We say that the impact of this voter is 1 because the difference between the two election outcomes, namely $\{A, B, C, D\}$ and $\{A, B, C, H\}$ is a single committee member. Using this strategy, we could compute the personal impact of each voter. Suppose the most significant personal impact is 2. We were able to compute the *personal impact index* (*PII*) to be 0.25, which is the ratio between the most significant personal impact and the size of the committee so that *PII* could be normalized to fall between 0 and 1.

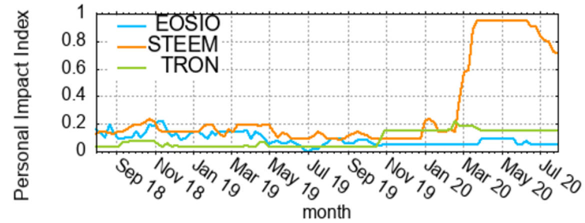

Figure 2: Personal impact index

A prerequisite to compute *PII* is the restoration of past election outcomes. On the basis of our datasets, we reconstruct daily election snapshots for all three blockchains. Specifically, on a daily basis, we first calculate the voting power of all voters and their voted candidates. We could then obtain the voting power received by each candidate and finally rank these candidates to identify the committee members. In this way, we could restore past election outcomes, compute the personal impact for each voter and obtain *PII*.

Results and insights. Fig. 2 shows the results of weekly *PII* measured in EOSIO, Steem and TRON from August 2018 to July 2020. Our study reveals that, before February 2020, a single voter in EOSIO, Steem and TRON can influence up to twenty percent of committee members. Specifically, in EOSIO, *PII* peaked in November 2018, then gradually decreased and remained low after November 2019. In contrast, in TRON, *PII* was initially low, then jumped abruptly in November 2019 and stayed high thereafter. In Steem, *PII* continued to remain at a high level. In March 2020, the month of TRON's takeover of Steem, we note that *PII* jumped to nearly 1, proving that the influence of a single voter nearly completely overturned the election outcomes.

Our findings suggest that personal impact is weakening in EOSIO but gradually rising in TRON. More importantly, our results validate our concerns. That is, a single entity could take over DPoS blockchains by exploiting the coin-based voting governance.

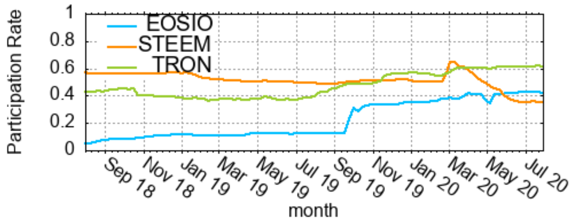

Figure 3: Participation rate

Participation in Governance

Participation in coin-based voting governance represents another critical dimension in characterizing the security of DPoS blockchains. We may imagine two extreme scenarios. In the first scenario, 95% of the total supply of coins has been frozen, converted into voting power and assigned to votes. In the second scenario, only 5% of the total supply of coins has been used in the election of committee members. There may be a higher degree of uncertainty about unused coins. That is, if a single entity controls these coins, the entity may be able to reverse election outcomes. From this perspective, the DPoS blockchain in the first scenario is more secure than the one in the second scenario. In the first scenario, even if all 5% unused coins are utilized to reverse the election outcomes, the 95% frozen coins make the blockchain highly resistant to takeovers. In contrast, in the second scenario, the 5% frozen coins imply that the blockchain is more vulnerable to takeovers.

Next, we present the metric, methodology, results and insights of the empirical study of the participation in coin-based voting governance in EOSIO, Steem and TRON.

Metric and methodology. We define a simple metric named *participation rate* (*PR*), which is the ratio between the frozen coins and the total supply of coins. A larger *PR* suggests that the DPoS blockchain network tends to be more resistant to takeovers. In comparison, a smaller *PR* indicates that the network tends to be more vulnerable to takeovers.

To compute *PR*, we need to obtain both the number of frozen coins and the daily supply of coins. We obtain information about frozen coins from our datasets' freezing and unfreezing operations. In addition, a large number of online exchanges provide data on the total supply of coins in EOSIO, Steem and TRON.

Results and insights. Fig. 3 presents the results of weekly *PR* measured in EOSIO, Steem and TRON from August 2018 to July 2020. We could see that EOSIO tends to have the lowest *PR* among the three blockchains. Interestingly, *PR* in EOSIO saw a surge in October 2019. After that, *PR* in EOSIO continued to rise and became higher than 40% in July 2020. In contrast, *PR* in both Steem and TRON tends to be relatively higher. In TRON, *PR* oscillated around 40% until August 2019. After that, *PR* in TRON climbed rapidly to 60%. To sum up, *PR* in both EOSIO and TRON showed an upward trend during the two years. However, *PR* in Steem continued to show a downward trend, with the exception of March 2020 (TRON's takeover of Steem), when a dramatic surge from approximately 50% to about 65% was observed.

Our results suggest that participation in governance in these three blockchains is generally low. This situation is getting better in EOSIO and TRON but is getting worse in Steem. More importantly, our results may indicate that 15% of the total supply of coins was used to take over Steem, which confirms our concern about unused coins.

Related Work

Recently, many blockchains based on DPoS consensus protocols have gained a lot of attention. However, the research on analyzing the performance and security of DPoS blockchains is still in the early stage. In 2019, Kwon et al. studied the degree of decentralization of various PoW, PoS, and DPoS blockchains (Kwon et al. 2019). In 2020, Li et al. quantitatively compared the degree of decentralization in Steem and Bitcoin using the Shannon entropy (Li and Palanisamy 2020). Huang et al. characterized activities including money transfers, account creation and contract invocation in EOSIO and detected bots and fraudulent activity (Huang et al. 2020). In 2021, Guidi et al. analyzed the behaviors and social impact of committee members in Steem (Guidi, Michienzi, and Ricci 2021). In 2022, Liu characterized EOSIO and showed that EOSIO was gradually evolving from decentralization to oligopoly (Liu et al. 2022). Tang et al. identified several types of user collusion behavior in Steem (Tang, Ni, and Zhang 2022). To the best of our knowledge, our paper presents the first empirical study that characterizes the personal impact and participation in coin-based voting governance in DPoS blockchains.

Conclusion

This paper presents a large-scale empirical study of two critical characteristics, personal impact and participation, of three leading DPoS blockchains. Our results suggest that personal impact is weakening in EOSIO but is gradually rising in TRON. Meanwhile, the problem of the low participation rate is gradually improving in EOSIO and TRON but not in Steem. More importantly, our results show that a single entity could leverage unused coins to take over DPoS blockchains by exploiting coin-based voting governance. Our results suggest that high personal impact and low participation rate could potentially make DPoS blockchains vulnerable to takeovers. Our study provides novel insights into the potential security risks in coin-based voting governance of DPoS blockchains. We believe that our research can contribute to helping people from a variety of areas gain a grasp of the theory and actual use of coin-based voting governance and also develop more secure DPoS blockchains.

Acknowledgments

This work was partially supported by the Beijing Natural Science Foundation under Grant No. M22039 and 4212008, the National Natural Science Foundation of China under Grant No. 62202038 and 62272031, and the Fundamental Research Funds for the Central Universities of China under Grant No. 2022JBMC007. Runhua Xu is the corresponding author (runhua@buaa.edu.cn).

References

Croman, K.; Decker, C.; Eyal, I.; Gencer, A. E.; Juels, A.; Kosba, A.; Miller, A.; Saxena, P.; Shi, E.; Gün Sirer, E.; et al. 2016. On scaling decentralized blockchains. In *International conference on financial cryptography and data security*, 106–125. Springer.

Guidi, B. 2020. When blockchain meets online social networks. *Pervasive and Mobile Computing*, 62: 101131.

Guidi, B.; Michienzi, A.; and Ricci, L. 2021. Analysis of Witnesses in the Steem Blockchain. *Mobile Networks and Applications*, 26(5): 2099–2110.

He, N.; Zhang, R.; Wang, H.; Wu, L.; Luo, X.; Guo, Y.; Yu, T.; and Jiang, X. 2021. {EOSAFE}: Security Analysis of {EOSIO} Smart Contracts. In *30th USENIX Security Symposium (USENIX Security 21)*, 1271–1288.

Huang, Y.; Wang, H.; Wu, L.; Tyson, G.; Luo, X.; Zhang, R.; Liu, X.; Huang, G.; and Jiang, X. 2020. Understanding (mis) behavior on the eosio blockchain. *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, 4(2): 1–28.

Kwon, Y.; Liu, J.; Kim, M.; Song, D.; and Kim, Y. 2019. Impossibility of full decentralization in permissionless blockchains. In *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*, 110–123.

Larimer, D. 2014. Delegated proof-of-stake (dpos). *Bitshare whitepaper*.

Li, C.; and Palanisamy, B. 2019. Incentivized blockchain-based social media platforms: A case study of steemit. In *Proceedings of the 10th ACM conference on web science*, 145–154.

Li, C.; and Palanisamy, B. 2020. Comparison of decentralization in dpos and pow blockchains. In *International Conference on Blockchain*, 18–32. Springer.

Li, C.; Palanisamy, B.; Xu, R.; Xu, J.; and Wang, J. 2021. SteemOps: Extracting and analyzing key operations in steemit blockchain-based social media platform. In *Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy*, 113–118.

Liu, J.; Zheng, W.; Lu, D.; Wu, J.; and Zheng, Z. 2022. From Decentralization to Oligopoly: A Data-Driven Analysis of Decentralization Evolution and Voting Behaviors on EOSIO. *IEEE Transactions on Computational Social Systems*.

Lin, Q.; Li, C.; Zhao, X.; and Chen, X. 2021. Measuring decentralization in bitcoin and ethereum using multiple metrics and granularities. In *2021 IEEE 37th International Conference on Data Engineering Workshops (ICDEW)*, 80–87. IEEE.

Nakamoto, S. 2008. Bitcoin: A peer-to-peer electronic cash system. *Decentralized business review*, 21260.

Tang, H.; Ni, J.; and Zhang, Y. 2022. Identification and Evolutionary Analysis of User Collusion Behavior in Blockchain Online Social Medias. *IEEE Transactions on Computational Social Systems*.

Wood, G. 2014. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151: 1–32.

Zheng, W.; Zheng, Z.; Dai, H.-N.; Chen, X.; and Zheng, P. 2021. XBlock-EOS: Extracting and exploring blockchain data from EOSIO. *Information Processing & Management*, 58(3): 102477.