Paper type | Received Day Mon Year; Accepted Day Mon Year; Published Day Mon Year
https://doi.org/10.55092/aiasxxxx

Blockchain Trilemma: The Measurements of Decentralization, Efficiency and Security

The title should be concise, informative and meaningful. It should include key terms to make it easier to be found via searching. Please avoid long systemic names, obscure abbreviations, acronyms or symbols or formulas. Avoid phrases such as “on the”, “a study of”, “research on”, “report on” “regarding”, and “use of”, omit “the” at the beginning of the title.

First Name Last Name[1], First Name Last Name[2] and First Name Last Name[3,4]*

[1]Institution, City, Country
[2]Institution, City, Country
[3]Institution, City, Country
[4]Institution, City, Country
Institution, City, Country (when only one institution)

Note: Pease list all authors’ full names and institutions. If an author’s current address is different from the address where the work was carried out, please add note. The general note symbol should be used in the following order: *,†,‡,§,¶,**,††,‡‡. Author Contribution: we encourage authors to make specific attributions of contribution and responsibility in the acknowledgements of the article, otherwise all co-authors will be taken to share full responsibility for all of the paper. Authors may wish to use a taxonomy such as CRediT to describe the contributions of each author.

* Correspondence author(s); E-mail: E-mail1, E-mail2

Abstract: Algorand and Beaconchain are both significant implementations of Proof of Stake (PoS)-based blockchain systems. Despite numerous experiments conducted in current research to analyze PoS systems, the quantification of various blockchain indicators remains unresolved. One of the most notable issues is the "Blockchain Trilemma" [1], which involves achieving a balance among decentralization, scalability, and security. To address the trilemma effectively, it is crucial to determine how to quantify and evaluate a blockchain system. Therefore, this article presents a comparative study of the Algorand and Beaconchain systems, with the aim of validating and proposing methods to quantify the components of the blockchain trilemma. We first analyze two practical blockchain systems as examples, categorizing the challenges into three dimensions. Second, we discuss existing research solutions for each dimension and propose our envisioned resolutions. Finally, leveraging existing data from the two blockchain systems, we substantiate our proposed solutions and explore their future developments.

Keywords: Blockchain trilemma ,PoS protocol, Algorand, Beaconchain.

1. Introduction

Recent years have witnessed the rapid development of blockchain. As a promising decentralized technique, blockchain has the potential of contributing to a more powerful distributed artificial intelligence. However, the enhancements of blockchain systems still rely on the "Blockchain Trilemma", in which an ideal blockchain needs to reach a balance of decentralization, scalability and security. Past researches have proposed different methods to quantify these three metrics. But most of them are built-up on the basis of blockchain 1.0[2], which may not perfectly match the trend of quick shifting from 1.0 to 2.0, represented by the Ethereum switching from Proof-of-Work(PoB) to Proof-of-Stake(PoS) community.

Motivated by this, in our work, we will explore the quantifications of decentralization, scalability and security with the data from two PoS based systems: (1) Algorand[3] and (2) Beacon Chain[4]. More specifically, our research will answer the following questions:

- How to Measure the Decentralization of Algorand and Beacon Chain?
- How to Measure the Scalability of Algorand and Beacon Chain?
- How to Measure the Security of Algorand and Beacon Chain?

For each question, we will further analyze in different methods with real-world examples: (1) For decentralization, we will conduct evaluation with mathematical coefficients to examine decentralization in different layers; (2) For scalability, we will discuss the insights drawn from real-world data and analyze the comparison between two blockchain systems; (3) For security, we summarize the potential threats and compare the reliability against various attacks. More specifically, in section II, we firstly offer a literature overview to summarize current works related to our research. Then in section III, we introduce our empirical data and provide detailed descriptions on our methods. Section IV illustrates our results for each question and Section V draws a conclusion of our findings with future extensions. We hope our research can contribute to a more efficient method of quantifying vital metrics for blockchain systems, building up a solid basis for further researches.

2. Related Work

In this section, we firstly provide a brief introduction of Algorand and Beacon Chain. Then, the following part will summarize exsiting works on blockchain metrics.

Algorand and Beacon Chain: As Proof-of-Stake(PoS) protocol tends to be a more efficient and energy-saving alternative of conventional Proof-of-Work(PoB) protocol, it is vital for us to testify proper methods to evaluate the improtant metrics for PoS based system. However, despite building up blockchain systems based on PoS protocol, there are currently various implementations.

Among them, two representative blockchains are Algorand and Beacon Chain. Algorand presents a novel consensus algorithm that combines PoS and Verifiable Random Function(VRF), enabling all participants to stake their tokens and actively involve in all blockchain activities. On the other hand, Beacon Chain adopts a PoS based consensus mechanism, where participants have to stake a required amount of tokens("stake") and obtain the authority of validation after a series of verifications. Thus, by comparing their metrics, we can have a deeper understanding of PoS based mechanism and furthermore, we can obtain a comprehensive study on quantifications of blockchain metrics.

Decentralization: Current studies have introduced many mathematical methods to quantify the decentralization by using various coefficients. In conventional understanding, decentralization refers to the absence of central coordination. Existing studies[5] claim that the decentralization in blockchain system is far more complex than conventional concept and further divide the blockchain decentralization into following categories: (1) Hardware; (2) Software; (3) Network; (4) Consensus; (5) etc. And some indices are also proposed and evaluated[6] on case studies accordingly, including Shannon Entropy, Gini Coefficient, Nakaoto Coefficient and Herfindahl-Hirschman Index.

Scalability: Scalability has always been a focal property in blockchain research. Generally, scalability is concerned with the overall efficiency of blockchains, where better scalability indicates less resource cost in blockchain transaction.[7]. A case study[8] is conducted on Bitcoin as an instance, in which a set of metrics are proposed to evaluate the scalabilty including the maximum throughput, latency, cost per transaction. A further extension[9] reveals that among those metrics, the maximum throughput and cost per transaction are considered the key components for quantifying the scalability of blockchain.

Table 1. Data Form for Beacon Chain

Data Type	Data Frame	Description
Block	Daily Block Count	Number of blocks produced per day
	Average Block Time	Average consensus time per block
	Average Gas Used by Blocks	Average gas used per block
Transaction	Transaction Count	Transaction count per day
	Gas Limit	Gas limit amout per day
	Burned Fees	Used tokens for transaction per day
Account	Validator Count	Validator counts per day
	Average Validator Balance	Average account balance of validators per day
	Participation Rate	Overall participation rate per day
Network	Network Liveness	Block count for confirmation

Security: Security is a core property of a blockchain system, since blockchain derives from a distributed ledger which emphasizes much on reliability and security. Based on the conventional concept, the security issues can be categorized into[10]: (1) 51% Attacks; (2) Forking Issue; (3) Eclipse Attacks; (4) etc. A further exploration[2] reveals that security issues in blockchain are complicated and can be roughly concluded into sub-categories by their causes including operation mechanism and smart contracts. However, current studies cannot present a comprehensive summarization of evaluating security. In contrast, most of the efforts are concentrated on the techniques to enhance the security of blockchain on the basis of real-world attacks such as the famous "DAO" attack. It is crucial for researchers to find efficient methods to evaluate the security capacity in order to prevent potential threats for a blockchain system.

3. Methodology

In this section, we will present our research methodology in details. First of all, we provide description on our real-world-dataset, where we will further explain our empirical data collection. Following the questions mentioned before, we will expand our study as solutions to those questions.

3.1. Data Description

We query data of Algorand and Beacon Chain in two methods. For Alogrand, we acquire data from BitQuery[11], where we query data by open APIs to pull on-chain data into our database. For Beacon Chain, we query data from Beacon Explorer[12] by using SIPDER framework.

In general, we collect on-chain data for both Algorand and Beacon Chain including block data and transaction data. Here, we give a more specific explanation on our dataset. As our interest is to analyze the mechanism performances of blockchain system, our task is more related to transactions and smart contracts data. For Beacon Chain, we query the website and parse the source code obtained to filter out recorded data. Then, we further categorize those data according to metrics we aim to quantify and the details are shown in table 1. For Algorand, we mainly query data through open APIs. However, due to the limitations of explorer adn APIs, the obtained data is less complex. Following the same step, we categorize the data according to our target metrics and the details are shown in table 2.

3.2. Solution I: Quantifications of Decentralization

Compared to the conventional concepts of decentralization study, we mainly focus on the impacts caused by consensus mechanisms. More specifically, the consensus mechanisms will influence PoS based blockchain systems in: (1) Consensus Layer; (2) Transaction Layer, because the on-chain activities are mainly determined through consensus protocol so that

Table 2. Data Form for Algorand

Data Type	Data Frame	Description
Block	Block Info Proposer Count	Block timestamp, address, height Proposer count per day
Transaction	Transaction Count Burned Fees	Transaction count per day Tokens used for transaction
Account	Block Reward	Reward for block proposal per day
Contract	Contract Calls Unique Calls	Overall contract calls per day Unique contract calls

each transaction could be authorized by all participants/validators. For each layer, we have:
Consensus Layer: We determine that the decentralization in PoS protocols is featured by the staking or voting process. The staking or voting process can be then represented by the proposer/validator data, where we consider the daily data as a unit and explore its relationship with the overall data.
Transaction Layer: Since only few existing works discuss the measurement of transaction layer, we here determine the transaction decentralization as the eveness of transactions across users[6]. On the basis of our dataset, we consider the daily transaction relevant data shown in table 1 and 2 as a unit for further analysis.

Therefore, in our study, we compare the decentralization in consensus level and transaction level. And for each layer, we introduce the indices based on the following coefficients to quantify the decentralization in multi-dimensions: (1) $Shannon\ Entropy$; (2) $Gini\ Coefficient$; (3) $Nakaoto\ Coefficient$ and (4) $Herfindahl\ Hirschman\ Index$.

Indice I: We firstly introduce the indice based on $Shannon\ Entropy$. As the entropy is always used to measure the randomness or chaos in a system, the proposed indice aims to measure the degree of randomness in the distribution of controllers. A higher value indicates more chaos in authority distribution while a lower value refers to a more centralized system. We define the indice $H(v)$ as:

$$H(v) = \prod_{i=1}^{N} P(v_i)^{-P(v_i)} \tag{1}$$

where the v_i refers to the unit data for each layer and the $P(v_i)$ refers to the weight of the unit data in respect to the overall dataset:

$$P(v_i) = \frac{v_i}{\sum_{i=1}^{N} v_i} \tag{2}$$

Indice II: We then introduce the second indice based on $Gini\ Coefficient$. As a classical economy indice, the $Gini\ Coefficient$ usually serves as an indicator of the wealth distribution within a given population. Thus, we still consider the P_i as the weight of a unit data in respect to complete dataset and define the indice II as:

$$G = 1 - \sum_{i=1}^{N} P_i^2 \tag{3}$$

where a higher indice value indicates less eveness in distribution of decentralization while a lower value shows more decentralization.

Indice III: The $Nakaoto\ Coefficient$ is utilized in various scenarios to measure the smallest number of entities that compromise a certain target. For instance, the coefficient is used in Bitcoin analysis to observe the mining power distribution. Here, we suppose that the smallest number of transaction entity or proposer/validator entity to accumulate 51% of the blockchain can present the decentralization in our target layers. Thus, we give the following definition:

$$N = min\{k \in [1, ..., K] : \sum_{i=1}^{K} P_i > 0.51\} \tag{4}$$

where the P_i refers to the weight of a unit data. In this case, a higher value means better decentralization, for there will need more entities to achieve the 51% of the whole system, and a lower value indicates more centralization on the contrary.

Indice IV: The $Herfindahl\ Hirschman\ Index$ is originally used to measure the concentration of market where different firms co-exist. From our perspective, the HHI indice can describe the decentralization for every data unit. Thus, we give the definition:

$$HHI = \sum_{i=1}^{N} P_i^2 \tag{5}$$

where the P_i indicates the share of each unit data in respect to overall dataset. In this case, a lower value refers to more decentralization while a higher one indicates more centralization.

3.3. Solution II: Evaluation of Scalability

Scalability here mainly refers to the capability of blockchain systems in throughput, latency, cost for transactions etc. Although existing works have attempted to measure the scalability of blockchain systems in various aspects, the quantification methods are still largely absent in current researches. Based on the matter of fact, we aim to conduct empirical analysis according to our real-world dataset.

More specifically, since we mainly focus on the consensus mechanism, the related metrics fall on the maximum throughput and latency. We design our research on scalability in a comparison analysis, where we categorize the targets into three dimensions related to our dataset:

- $Throughput$: We here define the throughput as the transaction counts for blockchain systems, since the consensus mechanism mainly affects the transaction procedures. We compare the daily transation data for Algorand and Beacon Chain, with more effort on the maximum of throughput to examine the reliability under extreme pressure.
- $Latency$: We define the latency as the time cost of block production and transaction confirmation. We illustrate the difference in average block time and transaction time to further compare the overall latency. A notable observation is that for Algorand, we calculate the average block time based on the timestamp and height, since the data form is different.

Generally, we suppose that better scalabilty will need better throughput behaviour and lower latency.

3.4. Solution III: Evaluation of Security

Security is always considered as a core property for blockchain systems. However, due to the speciality of security, it is usually difficult to measure this metric through mathematical tools or data analysis to gain a general understanding. Thus, we divide our exploration on security into two aspects: (1) Real Data Analysis; (2) Theoretical Comparison.

Real Data Analysis: Although it is hard to coordinate the ambiguous concept with the real world data, the reward mechanism in consensus still offers some hint for us. As is mentioned before, Algorand and Beacon Chain adopt different methods to implement PoS protocol. The implementations then lead to different designs for reward. Reward is usually distributed to proposers/validators as motivations to foster the users' willingness to preserve the blockchain community. Thus, we suppose that reward data can represent the security, where a higher reward will motivate more users to protect their community resulting in a more secure blockchain system.

However, due to the heterogeneity of data frames in our dataset, the reward data cannot directly obtained. Inspired by this dilemma, we propose to use the burned fees data as an indicator, since the reward is always reproduced from transaction cost for a mining-free blockchain system. Generally, a higher burned fees may potentially lead to more reward, but we can only obtain a rough trend rather than precise results due to absence of powerful supporting materials.

Theoretical Comparison: For this part, we mainly compare the resistance against common attacks in literature. As Algorand and Beacon Chain deploy different mechanisms for consensus stage, the capacity of resisting cyber attacks varies.

Algorand mainly relies on the VRF with simple reward mechanism, which provides an efficient proof token for certification and validation. On the other hand, Beacon Chain adopts a more complicated design with RANDO to handle the malicious behaviours. To present our analysis more clearly, we first pose an empirical scenario of classic 51% attack to analyse the robustness of Algorand and Beacon Chain on consensus level. Then, we explore more in-depth on their randomness, which is a key character for blockchain security.

4. Results

In this section, we present our empirical results and conduct comprehensive analysis of the results to reveal the insights obtained from our empirical evaluations.

4.1. R1: Measurement of Decentralization

Here, we firstly reveal our results of indices on consensus layer and transaction layer in table 3 and then compare the results for further analysis.

On the consensus layer, the indice values show that Algorand tend to gain more decentralization than Beacon Chain in the distribution of voting authority, with higher Shannon Entropy and Nakamoto Coefficient and lower Gini Coeffient and HHI. The result is not surprising, since the design goal of Algorand claimed that the "blockchain trilemma" should be mitigated. However, taking a deeper dive into the protocol mechanism, we can see that the result indeed reveals the advantage of Algorand, where no pre-requirement is set for proposers and everyone on-chain can involve in the voting procedures. On the contrary, as Beacon Chain requires users to stake a certain amount of tokens(stake), the overall mechanism of validators is less flexible.

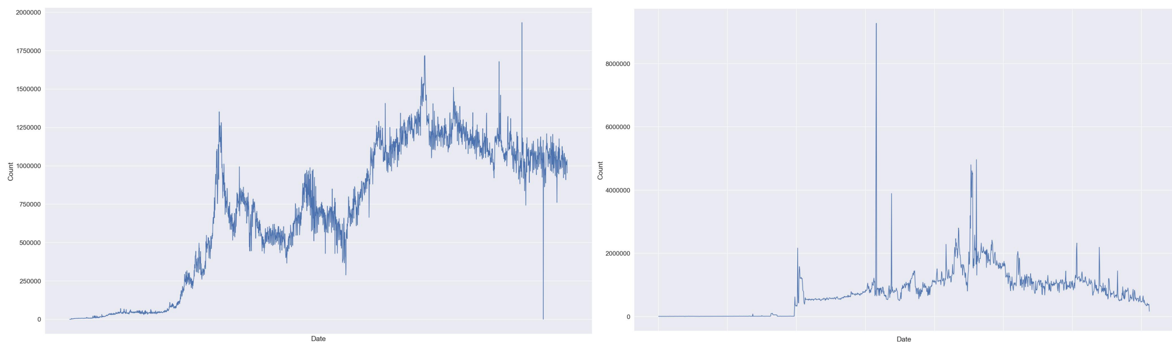
On the other hand, the results on the transaction layer present a mixed trend. Compared to the consensus layer, the Shannon Entropy and Nakamoto Coefficient are contradictory to the HHI and Gini Coefficient. The former reveals that Beacon Chain gains more decentralization while the latter shows that Algorand obtains more advantage. Due to Beacon Chain having been in existence for a longer period than Algorand, its transaction distribution may be influenced by transaction duration and total transaction volume, resulting in a more uniform distribution. However, this is not the case for Algorand. Due to its shorter transaction duration and lower visibility, its transaction volume tends to exhibit a less uniform distribution, with significantly higher transaction volumes during certain periods compared to others, which can be observed from Fig. 1. In a word, it still needs further experiments by controlling the environment factors to test out transaction decentralization of both blockchains.

4.2. R2: Evaluation of Scalability

The Fig. 1 illustrates the throughput(transactions) of Algorand and Beacon Chain. We can conclude that the overall transaction volume of Beacon Chain is much grater than Algorand. This is not surprising since the Beacon Chain, which is the key component of ETH 2.0, enjoys more popularity in cryptocurrency market. However, if we focus on the peak volume of daily

Table 3. The Decentralization Indices for Layers

Blockchain	Consensus Layer		Transaction Layer	
Algorand	Shannon Entropy	1364.34	Shannon Entropy	920.192
	Gini Coefficient	0.155	Gini Coefficient	0.155
	Nakamoto Coefficient	821	Nakamoto Coefficient	931
	Herfindahl Hirschman Index	0.0005	Herfindahl Hirschman Index	0.00015
Beacon Chain	Shannon Entropy	866.759	Shannon Entropy	2252.60
	Gini Coefficient	0.301	Gini Coefficient	0.301
	Nakamoto Coefficient	705	Nakamoto Coefficient	2067
	Herfindahl Hirschman Index	0.0021	Herfindahl Hirschman Index	0.0004



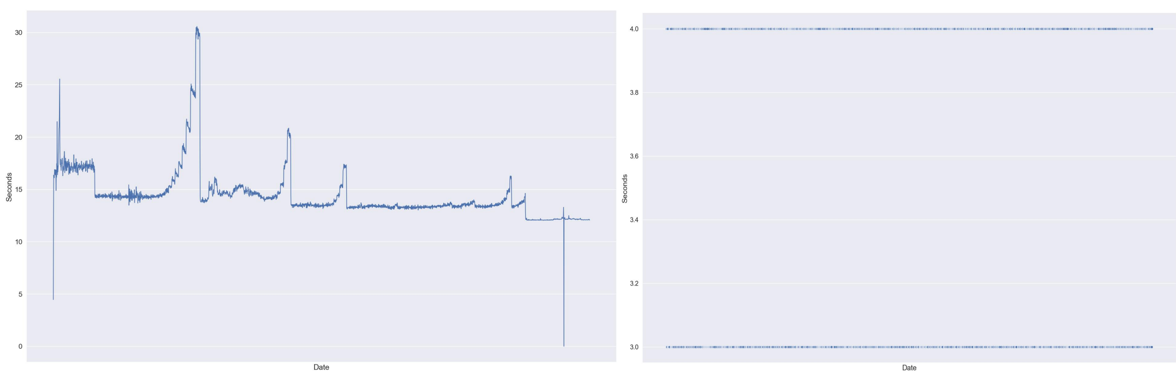
(a): Transaction of Beacon Chain (b): Transaction of Algorand

Figure 1. The Daily Transaction Data of Beacon Chain and Algorand

transactions, it can be observed that the maximum throughput of Algorand is 9271981 while the maximum throughput of Beacon Chain is 1932226. The peak volume of Algorand exceeds that of Beacon Chain, which is much astonishing since the Beacon Chain is a more popular and reliable community. Thus, we can roughly conclude that under extreme pressure, Algorand may handle more transactions than Beacon Chain.

From Fig. 2 we can see the latency behaviour of Algorand and Beacon Chain. Generally, the latency data shows a more stable trend for either Algorand and Beacon Chain compared with the transaction data. Furthermore, the average block time of Algorand is 3.5s. The average block time of Beacon Chain is 14.42s. A key observation is that the average block time and transaction time of Algorand is much shorter than Beacon Chain, which means Algorand can produce new blocks and confirm them with less time.

Therefore, we can draw a general conclusion that Algorand is somehow more capable of scalability, with larger transaction peak volume and shorter time cost for blocks and transactions. However, due to the different market scales, the block counts and transaction amounts are at different levels for Algorand and Beacon Chain, which may cast more uncertainty on



(a) Avg Block Time of Beacon Chain (b) Avg Block Time of Algorand

Figure 2. The Avg Block Time of Beacon Chain

analysis of their daily blcok and transaction data. Further evaluations are still needed to obtain more precise observations for scalability.

4.3. R3: Analysis of Security

Real Data Analysis: Compared to the earlier metrics, security is always crucial but more abstract metric. To gain a more comprehensive understanding, we firstly provide some empirical data analysis. The average burned fees per day of Beacon Chain is 4690.36, while that of ALgorand is 947.124. It can be clearly observed that Beacon Chain requires more fees for transactions. According to the Honest Majority Money(HMM)[13] hypothesis, if the majority of the system tends to remain honest, the security of the system will be guaranteed since the majority seems to be more likely to protect the community. In addition, the main driving point for users to protect their community is the on-chain reward. Hence, with a greater reward, the Beacon Chain may gain more security in long-term.

Theoretical Comparison: Given the scarcity of recorded attacks on both Algorand and Beacon Chain, we present a brief comparison of their mechanisms in the face of the classic 51% attack[14]. The 51% attack typically involves malicious nodes gaining control of 51% of the resources in a given community.

In our scenario, the hypothesis is that attackers hold 51% of the voting power in the consensus stage, for instance, 51% of validators/proposers are under the control of attackers. In this case, attackers can predict the next proposal, thereby controlling the overall behavior of the blockchains.

To mitigate this kind of attack, enhancing randomness is an effective method, making it challenging for attackers to predict the next chosen block. Algorand achieves this by implementing a random seed Q[15], while Beacon Chain adopts a random function called RANDO[16]. The random seed Q in Algorand is independent of transactions and updates in each round of voting. This ensures randomness with no intersection between transactions and the random seed, unaffected by the number of transactions. Compared with Algorand, RANDO in Beacon Chain is more straightforward. To maintain randomness, the rand value in each round is accumulated with the former rand value, typically realized by an "XOR" function that mixes the timestamp with the random value.

Here, we delve deeper into their bias in randomness. The 51% attack usually refers to the takeover of blockchains, but an interesting observation is that the takeover is considered infeasible in both [15] and [16]. For Beacon Chain, accumulating 51% of the overall stake is considered impossible, assuming any attacker will obtain less than half the stake. Thus, the 51% attack is not feasible in Beacon Chain. However, for Algorand, the credentials for the election or choice of blocks are considered as evenly distributed "lottery," where each "lottery" maintains the same probability of being chosen with a temporary key. Once the consensus procedure is confirmed, the key is destroyed. Therefore, with equally distributed credentials and ephemeral keys, the randomness may not bias for any participant, and even if there are corruptions in the blockchain, the temporary key still maintains robustness.

In summary, both Algorand and Beacon Chain demonstrate good randomization and robustness in literature analysis, but further empirical analysis is still required for a more precise comparison.

5. Conclusion

In this article, we summarize current works on quantifying metrics for decentralization, scalability and security in blockchains. Based on existing works, we conduct experiments and analysis on our real-world dataset of Algorand and Beacon Chain, to further find out effective quantifications for blockchain 2.0.

In perspective of Decentralization, we compare the two blockchains in two layers, Consensus Layer and Transaction Layer, to evaluate and analyze the decentralization. For each layer, we mainly utilize four indices to quantify decentralization on real-world data. From the results, we find that the Algorand gains more decentraliztion than Beacon Chain, which conforms to the design goal of Algorand.

For scalability, we focus on the throughput and latency. By analyzing the throughput and latency related data in our dataset, we compare the data and observe that Algorand maintains more scalability than Beacon Chain in some extend. However, current data may not perfectly support our insights due to lots of interference factors. Further simulations are still necessary for comparisons.

In analysis of security, we attempt to conduct empirical comparisons with real-world data and we also commit theoretical analysis of their robustness against typical takeover attack, the 51% attack. From real-world data comparison, we mainly compare the burned fees which is a main source of reward in blockchain systems. The result reveals that the participants in Beacon Chain can obtain more rewards because of more burned fees, which is a good sign for long-term security in the future. From the theoretical analysis, we can conclude that the robustness against biasability is theoretically sound. However, exploration for security requires more specific simulations to provide more convincing details.

Future work is ahead.

References

[1] Buterin V. On Public and Private Blockchains. https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains.

[2] Li X, Jiang P, Chen T, Luo X, Wen Q. A survey on the security of blockchain systems. *Future generation computer systems* 2020 107:841–853.

[3] Chen J, Micali S. Algorand: A secure and efficient distributed ledger. *Theoretical Computer Science* 2019 777:155–183.

[4] Grandjean D, Heimbach L, Wattenhofer R. Ethereum Proof-of-Stake Consensus Layer: Participation and Decentralization. *arXiv preprint arXiv:2306.10777* 2023 .

[5] Karakostas D, Kiayias A, Ovezik C. SoK: A Stratified Approach to Blockchain Decentralization, 2022.

[6] Zhang L, Ma X, Liu Y. SoK: Blockchain Decentralization, 2023.

[7] McCorry P, Buckland C, Yee B, Song D. Sok: Validating bridges as a scaling solution for blockchains. *Cryptology ePrint Archive* 2021 .

[8] Croman K, Decker C, Eyal I, Gencer AE, Juels A, *et al.* On Scaling Decentralized Blockchains. In *Financial Cryptography and Data Security*, Clark J, Meiklejohn S, Ryan PY, Wallach D, Brenner M, *et al.*, eds., Berlin, Heidelberg: Springer Berlin Heidelberg2016 pp. 106–125.

[9] Zhou Q, Huang H, Zheng Z, Bian J. Solutions to Scalability of Blockchain: A Survey. *IEEE Access* 2020 8:16440–16455. 10.1109/ACCESS.2020.2967218.

[10] Islam MR, Rahman MM, Mahmud M, Rahman MA, Mohamad MHS, *et al.* A review on blockchain security issues and challenges. In *2021 IEEE 12th Control and System Graduate Research Colloquium (ICSGRC)*, IEEE2021 pp. 227–232.

[11] https://bitquery.io.

[12] https://beaconcha.in/.

[13] Gilad Y, Hemo R, Micali S, Vlachos G, Zeldovich N. Algorand: Scaling Byzantine Agreements for Cryptocurrencies. In *Proceedings of the 26th Symposium on Operating Systems Principles*, New York, NY, USA: Association for Computing Machinery2017, SOSP '17 p. 51–68. 10.1145/3132747.3132757.

[14] Oksiiuk O, Dmyrieva I. Security and privacy issues of blockchain technology. In *2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, IEEE2020 pp. 1–5.

[15] https://github.com/algorandfoundation/specs/tree/.
[16] https://eth2book.info/capella/part2/building_blocks/randomness/.