IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 4 May 2024, accepted 30 May 2024, date of publication 5 June 2024, date of current version 14 June 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3410025

RESEARCH ARTICLE

A Formulation of the Trilemma in Proof of Work Blockchain

TAISHI NAKAI[1], AKIRA SAKURAI[1], SHIORI HIRONAKA[2], AND KAZUYUKI SHUDO[2], (Senior Member, IEEE)
[1]Graduate School of Informatics, Kyoto University, Kyoto 606-8501, Japan
[2]Academic Center for Computing and Media Studies, Kyoto University, Kyoto 606-8501, Japan

Corresponding author: Taishi Nakai (distributed.nakai@gmail.com)

This work was supported by the Japan Society for the Promotion of Science (JSPS) KAKENHI under Grant JP21H04872 and Grant JP24H00691.

ABSTRACT The blockchain trilemma, introduced in 2017 on a blog post authored by Vitalik Buterin, one of Ethereum's co-founders, asserts that achieving decentralization, scalability, and security simultaneously within a blockchain is unattainable. While this concept has garnered empirical support through extensive analyses of blockchain performance, it remains unproven theoretically. In this study, we establish a formula representing the trilemma within a Proof of Work blockchain and validate it through theoretical and experimental analyses. Additionally, we explore the correlation between a formula term denoting decentralization and established decentralization indices, finding a strong correlation with the Herfindahl–Hirschman Index. Moreover, our analysis reveals that strategies to enhance trilemma properties within the trilemma's constraints can be classified into two distinct categories. The first strategy is to reduce the block header or transaction size. The second strategy is to optimize the propagation time per byte between nodes.

INDEX TERMS Blockchain, decentralization, scalability, security, trilemma.

I. INTRODUCTION

A. BACKGROUND

1) PROOF OF WORK BLOCKCHAIN

Blockchain, a distributed ledger system, gained significant attention in 2008 with the publication of Satoshi Nakamoto's paper on Bitcoin [1].

In blockchain systems, transactions are processed in units called ''blocks.'' Each block contains a header and multiple transactions. If the hash value of the header is below a certain target, the block is considered valid. The process of finding this header is referred to as mining. Nodes that participate in this process and generate blocks are called miners. Miners with greater computational power are more likely to produce blocks. Once a block is generated, it is disseminated through the network to other miners. If other miners verify the block and deem it valid, the miner who produced the block receives a reward. Additionally, this entire process is called Proof of Work (PoW).

The associate editor coordinating the review of this manuscript and approving it for publication was Barbara Masini.

Each block includes reference information to the previous block. The series of linked blocks formed by this reference structure is called a chain. Occasionally, the chain may split into two branches, a situation known as a fork. In such cases, to converge on a single chain, miners select the longest chain, a principle known as the longest chain rule.

2) SCALABILITY PROBLEM

Blockchain provides high decentralization, but it has had a problem with low processing performance (Scalability) since the emergence of Bitcoin. In fact, Bitcoin operates with a low performance of 7 TPS (transactions per second), which is a known scalability problem. This is one of the major challenges in blockchain and causes a surge in transaction fees. As a result, it has prevented Bitcoin from becoming widespread as an everyday payment system and made it difficult to apply blockchain technology outside of cryptocurrencies, such as agriculture, medical, and supply chain [2], [3], [4].

Therefore, many studies have been conducted to improve processing performance, but most of these, intentionally

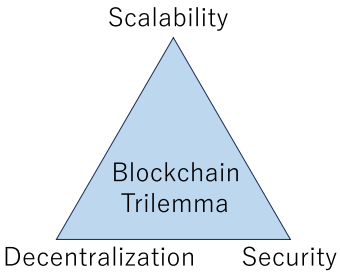


FIGURE 1. Blockchain trilemma.

or not, achieve higher performance at the expense of decentralization. In the case of permissioned blockchains like Hyperledger Fabric [5], trust in the operators is necessary. Although it is possible to have multiple operators, the system can only support up to around 100 nodes, not hundreds to thousands of nodes like Bitcoin or Ethereum. Furthermore, even blockchains that allow anyone to read the ledger, like Bitcoin and Ethereum, are not necessarily decentralized. For example, in Ripple's XRP Ledger [6], effectively only the 35 nodes listed on a list managed by Ripple itself (UNL) perform transaction validation. The mode of validation is similar to that of permissioned blockchains, so the number of nodes that can participate in validation cannot be significantly increased.

3) TRILEMMA

A critical challenge in blockchain technology is the "trilemma" first posited by Vitalik Buterin, one of Ethereum's [7] co-founders, in 2017 [8]. Buterin's concept stipulates that a blockchain network can, at best, achieve two out of the following three essential properties: decentralization, scalability, and security. This assertion, referred to as the blockchain trilemma, is depicted in Fig. 1.

The trilemma is merely a heuristic and has been considered correct in the midst of numerous analyses of blockchains. Therefore, there is no clear consensus on the definition of the three properties of the trilemma. The followings are a brief and intuitive definition of the three properties for blockchain consensus layer. Note that they are different from the Buterin's trilemma definition [8].

Decentralization
: The degree to which the influence of each node is distributed across the entire system [9], [10].

Scalability
: Transaction processing performance [11], [12].

Security
: The system is secure from attackers [13].

B. CHALLENGES

The empirical recognition of this trilemma in blockchain technology has been well-established through numerous analyses. However, its mathematical demonstration remains elusive, with only a theoretical exposition of the trade-off between scalability and security presented [14].

Given this lack of mathematical proof, the impact of scalability improvements on decentralization or security remains uncertain. Blockchain technology inherently suffers from lower scalability (throughput) compared to traditional databases, posing challenges for its application in industrial sectors [2], [3], [4]. Consequently, extensive research efforts have been dedicated to enhancing scalability [5], [6], [7], [15], [16], [17], [18], [19], yet the exact ramifications of decentralization and security remain unclear.

Furthermore, while Buterin's trilemma properties are defined in binary terms, they exhibit an inverse relationship in reality. For instance, according to Buterin, Bitcoin lacks scalability. However, compromising security or decentralization can lead to a proportional increase in scalability, challenging the strict binary interpretation of the trilemma.

In this study, we theoretically derive the formula that represents the blockchain trilemma. Specifically, we confirm, through theory and simulation experiments, that a particular term in the trilemma formula indicates decentralization by listing the necessary conditions for a decentralization index. Furthermore, we verify whether the trilemma formula holds on a simulator through experiments. We demonstrate that there are two ways to improve trilemma properties under the constraints of the blockchain trilemma, from the formula.

This research is expected to have a wide-ranging impact on the blockchain field in the future as follows:

- It will enable analysis of how previous scalability improvement methods and increases in the number of nodes in Proof of Work blockchains have impacted security and decentralization.
- If it does not violate the formula of the dilemma we present, it allows for proposals to enhance scalability, security, and decentralization without compromising these elements, and to improve other aspects in Proof of Work blockchains.
- This study could lead to the discovery of a formula representing the trilemma not only in Proof of Work but also in blockchains that use other consensus algorithms.

C. MAIN CONTRIBUTION

Our main contributions of this study are as follows:

1) We present a mathematical demonstration of the blockchain trilemma in systems employing Proof of Work, focusing on the architecture for the consensus layer. Our approach involves deriving a formula wherein the product of decentralization, scalability, and security, representing continuous variables rather than binary states, remains constant (Section II).
2) We highlight a specific term within the trilemma formula that represents the concept of decentralization. This representation is achieved through a comprehensive examination that encompasses both theoretical analysis and experimental validation (Section IV).
   a) Demonstrate that the increase or decrease in the term of the trilemma formula that includes decentralization is more significant with a smaller range of node numbers or with a larger range of bias (Section IV-C).

b) Indicate that the Herfindahl-Hirschman Index (HHI) is the most suitable existing decentralization index that meets the two conditions we propose for a decentralization index (Section V-B).
c) Show that the term in the trilemma formula that includes decentralization expresses decentralization in a form similar to the Herfindahl-Hirschman Index (HHI) (Section IV-B, V-C).

3) We confirm the validity of the trilemma formula through verification in a simulation environment (Section VI).
4) Utilizing the trilemma formula developed in our study, we illustrate two distinct approaches for enhancing trilemma properties while adhering to the constraints imposed by the trilemma (Section VII).

D. RELATED WORK

1) BUTERIN'S TRILEMMA

Buterin provided definitions for trilemma properties.

Decentralization
Decentralization is defined as the system being able to run in a scenario where each participant only has access to $O(c)$[1] resources, i.e. a regular laptop or small Virtual Private Server.

Scalability
Scalability is defined as being able to process $O(n) > O(c)$ transactions.

Security
Security is defined as being secure against attackers with up to $O(n)$ resources.

Here, c represents the size of computational resources (including computation, bandwidth, and storage) available to each node, and n refers to the size of the ecosystem in some abstract sense. It is assumed that transaction load, state size, and the market cap of a cryptocurrency are all proportional to n. With this definition, although Bitcoin attains decentralization and security, it faces limitations in scalability, accommodating only up to 27 transactions per second [20]. This is clearly below the number of transactions that a normal computer can process.

Buterin's trilemma properties have not been quantified and are expressed in binary terms. Moreover, decentralization is generally understood as the degree to which the influence of each node is distributed across the entire network. However, it is also perceived as indicating the ease of participation in the network. In this research, we present each property not in binary terms, but quantitatively. Furthermore, we interpret decentralization in a more general sense.

2) VARIOUS TRILEMA THREE PROPERTIES

Scalability, security, and decentralization definitions vary widely among individuals and are not universally adopted from Buterin's definitions.

[1] Buterin's use of the big O notation does not follow its standard definition. However, out of respect for the original text, we retain the notation O as presented.

For example, scalability often refers to the throughput of transactions writing, but can also include the throughput of data reading, the storage size needed for node construction, and bootstrap time [11], [12]. Security can be understood as confidentiality, integrity, and availability within the CIA Triad or as resilience against double spending and 51% attacks [21], the frequency of fork occurrences [14], [22]. Decentralization, according to Buterin's trilemma, has been defined as 'whether the system can be accessed with few resources' [8]. It has also been delineated in terms of structural, governance, and logical decentralization [23] by Buterin, the distribution of block generation numbers by Lin et al. [9], and five types of decentralization classified by Zhang et al.: consensus, network, wealth, governance, and transaction decentralization [10]. Moreover, various decentralization indices such as the Gini coefficient, Herfindahl–Hirschman Index, and Nakamoto coefficient are used in research [10].

In this paper, we focus on the architecture level of PoW blockchain for the consensus and define the three properties of the trilemma as follows: transactions per second, which indicates the throughput of transactions writing, as scalability; the inverse of the fork rate as security; and the hash rate distribution and number of nodes as decentralization. We present a mathematical formula for the trilemma incorporating these three properties. Additionally, since there is no established quantification for decentralization compared to scalability and security, we analyze the relationship between existing decentralization indices—Gini coefficient, HHI, Nakamoto coefficient—and the term representing decentralization in our formula.

3) SCALABILITY IMPROVEMENT RESEARCHES

We have already introduced some scalability improvement studies in Section I-A2. Here, we introduce further scalability improvement research. For example, Ethereum [7] aims to increase scalability by reducing the average block creation time. SPECTRE [15] utilizes a directed acyclic graph for its consensus algorithm to improve scalability. Additionally, Sharding, as seen in RapidChain [24], Monoxide [16], and CHERUBIM [17], distributes transactions across multiple groups of nodes to enhance scalability. Rollup [18] processes transactions off-chain to improve scalability. There are also studies, like Graphene [19], that aim to increase scalability by reducing the size of propagated blocks.

4) TRILEMMA RESEARCHES

There are some researches of trilemma. Werth et al. [21] summarized and compared the three properties of the trilemma across multiple consensus algorithms. However, they did not theoretically demonstrate that these three properties are in a trilemma relationship.

Some researchers try to break through the trilemma. Gilad et al. developed the blockchain Algorand [25], which adopts Proof of Stake (PoS) to resolve the trilemma [26].

Algorand increases scalability while avoiding forks, which can impact security. Algorand prioritizes PoS, but we prioritize PoW. The Trifecta Blockchain Team [27] presents Trifecta to resolve the trilemma by combining Prism [28] with Sharding. Prism maintains security by separating the chains that process transactions from those that achieve consensus, thereby providing high scalability. In this method, Prism, as described in our trilemma formula, is a technique used to improve scalability within the constraints of the trilemma (cf. Section VII-A). Wang et al. developed the permissioned blockchain GBT-CHAIN [29]. They defined the general properties of the trilemma (consistency, scalability, and partition tolerance) from the CAP theorem and attempted to solve the trilemma by quantitatively expressing these properties. While the GBT chain centers on a permissioned blockchain with a BFT Consensus algorithm such as Hotstuff, we focus on a permissionless blockchain with PoW.

There are studies that have theoretically demonstrated the trade-offs between two properties of the trilemma. Fujihara [14] presented a mathematical formulation showing the trade-off between transaction processing capacity (scalability) and fork rate (security). Chu and Wang [30] demonstrated mathematically that there is an upper limit to transaction processing capacity in decentralized ledgers, showing a trade-off between scalability and decentralization. Albrecht et al. [31] pointed out the trade-off between security (the likelihood of fork rates occurring) and decentralization (resistance to attacks when there are many nodes). However, neither paper simultaneously addresses all three properties of the trilemma, nor do they consider the distribution of hash rates, which is crucial for decentralization.

In this paper, we derive a formula where the product of three terms representing scalability, security, and decentralization equals a constant, thus illustrating the trilemma. Furthermore, we show that methods to improve trilemma properties under trilemma constraints can be classified into two categories by reducing values that are not directly related to the three properties, set as constants in the formula.

E. OUTLINE

The rest of this paper is organized as follows: Section II derive the formula that represents the blockchain trilemma. Section III shows that how the formula express ''Scalability'' and ''Security''. Section IV denotes that a specific term within the trilemma formula represents the concept of decentralization. Section V evaluates the validity of current decentralization indices according to the two conditions for a decentralization index we propose and analyze the relationship between the decentralization term in our formula and the existing indices. Section VI confirm the validity of the trilemma formula using a simulator. Section VII reveals that approaches to enhance trilemma properties within the trilemma's constraints can be classified into two distinct categories from the trilemma formula. Finally, we discuss the comparison with Buterin's trilemma and the analysis and open problems that are outside the scope of our assumptions for the trilemma formula in Section VIII.

This paper is an extended version of our previous work [32]. This paper shows a specific term within the trilemma formula represents the concept of decentralization by theory and simulation in Section IV. Moreover, we presents that among the three existing decentralization indices, the Gini coefficient, HHI, and Nakamoto coefficient, the HHI has the strongest relationship with the decentralization term in our trilemma formula in Section V. Furtheremore, we confirm the validity of the trilemma formula through verification using a simulator in Section VI.

TABLE 1. The symbols in our paper.

Symbol	Explanation
T_w	The average block propagation time weighted by the hash rate.
$T_{w,i}$	The average block propagation time weighted by the hash rate for node i. When node i generates a block, the time it takes for that block to reach all other nodes, weighted by the hash rate of the receiving node.
H_i	The proportion of the hash rate that node i possesses relative to the entire network's hash rate. $\sum_{i=1}^{n} H_i = 1$.
n	The number of nodes participating in the network. In our paper, "node" means "miner".
F	Theoretical fork rate.
T	Average block generation time.
T_{ij}	The time taken for the block generated by node i to propagate to node j
t_{ij}	The time taken for a block generated by node i to propagate to node j per byte is t_{ij}.
B	Block size. It is important to note that the block size refers not to the size of blocks included in the main chain, but to the size of the blocks when they are propagated for consensus.
B_h	The block header size.
B_{tx}	The size of one transaction.
n_{tx}	The number of transactions contained in one block.
$\boldsymbol{H}$	$\boldsymbol{H} = \begin{pmatrix} H_1 \\ H_2 \\ \vdots \\ H_n \end{pmatrix}$.
$\boldsymbol{P}$	$\boldsymbol{P} = \begin{pmatrix} 0 & t_{12} & \dots & t_{1n} \\ t_{21} & 0 & \dots & t_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ t_{n1} & t_{n2} & \dots & 0 \end{pmatrix}$.

II. MATHEMATICAL DESCRIPTION OF THE TRILEMMA

We formulate an equation, scalability $\times$ security $\times$ decentralization $=$ constant, by reformulating equations describing the average block propagation time weighted by the hash rate and the theoretical fork rate, as outlined in Sakurai et al.'s study [33].

First, we describe the condition for deriving the trilema formula in Section II-A. Second, we explain the definition of the average block propagation time weighted by the hash rate, denoted as T_w, in Section II-B. Subsequently, in Section II-C, we deduce the formula representing the trilemma from T_w and

theoretical fork rate F. The definitions of the symbols used are summarized in Table 1.

A. THE CONDITION FOR THE TRILEMMA FORMULA

Here, we describe the conditions for deriving our trilemma formula:

- The consensus algorithm is PoW.
- The fork choice rule follows the longest chain rule.
- Attackers do not exist. This means that it is not a situation where an attacker is actively attacking and nodes do not collude.
- All nodes are miners.
- Nodes are not grouped to process separate data in each group; that is, Sharding is not adopted, and all calculations are performed in a single shard.
- We do not consider off-chain transaction processing; that is, all transaction executions are considered on-chain.

We have set PoW and the longest chain rule following Bitcoin. When considering security, it is not assumed that an attacker is always attacking; rather, we consider whether an attack would likely be successful if it were to occur. Focusing on constraints at the consensus layer, we do not consider Sharding or off-chain channels, and think about the simplest scenario of a single shard and on-chain transaction processing.

B. THE AVERAGE BLOCK PROPAGATION TIME WEIGHTED BY THE HASH RATE

We elucidate the average block propagation time weighted by the hash rate, denoted as T_w, following the definition by Sakurai et al. [33]. First, we describe the average block propagation time weighted by the hash rate for node i, $T_{w,i}$.

$T_{w,i}$ represents the average block propagation time weighted by the hash rate when node i successfully generates a block. $T_{w,i}$, as defined by the following equation:

$$T_{w,i} = \int_0^\infty -t \cdot u_i'(t)dt \tag{1}$$

where $u_i(t)$ represents the total proportion of the hash rate of nodes that have yet to receive the block t units of time after node i's successful block generation. Furthermore, $u_i'(t)$ signifies the derivative of $u_i(t)$. In reality, $u_i(t)$ may not be differentiable, but for simplicity, $u_i(t)$ is treated as differentiable in this context.

Figure 2 presents a graph where the horizontal axis signifies the elapsed time t since block generation, and the vertical axis indicates the total hash rate of miners that have received the block up to time t. The average block propagation time weighted by the hash rate for node i, $T_{w,i}$, is depicted by the area of the red-shaded region on the graph.

In scenarios where not only node i but also other nodes generate blocks, the average block propagation time weighted by the hash rate, T_w, is calculated by taking the weighted average of each node's average block propagation time weighted by the hash rate with respect to each node's hash rate. Specifically, T_w is defined by the following equation:

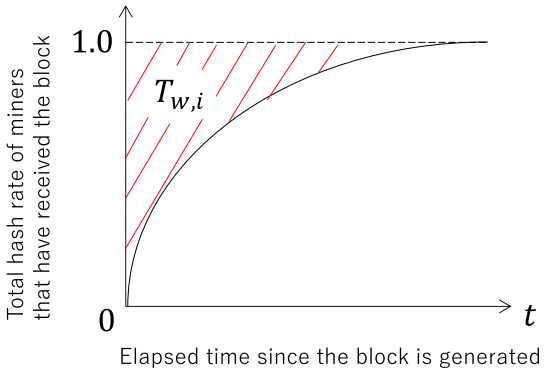


FIGURE 2. Visualization of $T_{w,i}$. The total hash rate of miners who have received the block before time t versus the elapsed time since the block is generated by node i. The area of the red shaded region corresponds to $T_{w,i}$.

$$T_w = \sum_{i=1}^{n} H_i \int_0^\infty -t \cdot u_i'(t)dt \tag{2}$$

where n represents the number of nodes participating in the network, and H_i signifies the proportion of the hash rate owned by node i relative to the hash rate of the entire network. Additionally, according to the definition of H_i, the following equation holds.

$$\sum_{i=1}^{n} H_i = 1 \tag{3}$$

C. DERIVATION OF THE TRILEMMA

Sakurai and Shudo [33] conveniently represented T_w as an integral. We provide a more accurate representation of T_w as the sum of discrete values and subsequently derive the formula representing the trilemma using this expression.

The average block propagation time weighted by the hash rate for node i, $T_{w,i}$ signifies the time taken for a block generated by node i to propagate to all other nodes, weighted by the hash rate of each receiving node. If T_{ij} represents the time taken for the block generated by node i to propagate to node j, then $T_{w,i}$ can be expressed as the follows. In this context, it is assumed that there is no block propagation from node i to itself.

$$T_{w,i} = \sum_{j=1, j\neq i}^{n} H_j T_{ij} \tag{4}$$

From $T_{w,i}$, we derive T_w. The probability of node i generating a block is determined by the ratio of node i's hash rate to the entire blockchain network's hash rate. Thus, from (4), T_w can be expressed by the following equation.

$$T_w = \sum_{i=1}^{n} H_i T_{w,i} \tag{5}$$

$$= \sum_{i=1}^{n} H_i \sum_{j=1, j\neq i}^{n} H_j T_{ij} \tag{6}$$

When B represents the block size and t_{ij} denotes the propagation time from i to j per byte when node i generates a block, (6) can be represented by the following expression.

$$T_w = \sum_{i=1}^{n} H_i \sum_{j=1, j\neq i}^{n} H_j \cdot B \cdot t_{ij} \tag{7}$$

$$= B \sum_{i=1}^{n} H_i \sum_{j=1, j\neq i}^{n} H_j t_{ij} \tag{8}$$

Because (7) is a quadratic form (a polynomial consisting only of quadratic terms), it can be represented using a vector $\boldsymbol{H}$ that is the distribution of hash rates and a matrix $\boldsymbol{P}$, whose elements represent the block propagation times between each pair of nodes.

$$T_w = B\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H} \tag{9}$$

Here, the vector $\boldsymbol{H}$ and the matrix $\boldsymbol{P}$ are represented as follows.

$$\boldsymbol{H} = \begin{pmatrix} H_1 \\ H_2 \\ \vdots \\ H_n \end{pmatrix} \tag{10}$$

$$\boldsymbol{P} = \begin{pmatrix} 0 & t_{12} & \dots & t_{1n} \\ t_{21} & 0 & \dots & t_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ t_{n1} & t_{n2} & \dots & 0 \end{pmatrix} \tag{11}$$

$\boldsymbol{H}^\top$ denotes the transpose of the vector $\boldsymbol{H}$. Within the matrix $\boldsymbol{P}$, the diagonal elements indicate the propagation time to the same node. Because no block propagates between identical nodes, these diagonal elements are assigned a value of 0.

The theoretical fork rate F, proposed by Sakurai et al [33], can be determined using the average block generation time T and the average block propagation time weighted by the hash rate T_w as follows. Note that this formula is valid under the assumption that no more than two blocks are produced at the same height.

$$F = \frac{T_w}{T} \tag{12}$$

Then, substitute (9) into (12).

$$F = \frac{B\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}}{T} \tag{13}$$

Moreover, the block size B can be expressed in terms of the block header size B_h, the size of a single transaction B_{tx}, and the number of transactions contained within one block n_{tx} as follows.

$$B = B_h + B_{tx} \cdot n_{tx} \tag{14}$$

The following formula can be derived by substituting (14) into (13) and transforming the equation under the condition $F \neq 0$.

$$\frac{B_h + B_{tx} \cdot n_{tx}}{T} \cdot \frac{1}{F} \cdot \boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H} = 1 \tag{15}$$

III. INTERPRETATION OF TRILEMMA FORMULA

We elucidate how the derived formula expresses the three properties of the trilemma—scalability, security, and decentralization (15).

In (15), the term $\frac{n_{tx}}{T}$ represents the number of transactions processed per unit of time, commonly known as transactions per second (TPS). TPS is a widely index for scalability [12]. Therefore, the first fraction includes a representation of scalability, assuming constants B_h and B_{tx} and TPS is a metric for scalability.

Moreover, a high fork rate complicates miners' decisions regarding which branch to adopt. This fragmentation of hash rate can increase security risks, such as Double Spending Attack and Selfish Mining [13]. Consequently, as the system becomes more susceptible to forking, it becomes more vulnerable to attacks. In fact, Fujiwara [14] and Zhu et al. [22] utilize the fork rate as a metric to evaluate security. Therefore, the inverse of the fork rate $\frac{1}{F}$ can be interpreted as a representation and index of security.

If B_h and B_{tx} are constants, and considering $\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}$ as a property for decentralization, equation (15) indicates that the product of the three factions representing scalability, security, and decentralization is equal to 1. This suggests that it is difficult to improve all three elements simultaneously, which is the essence of the trilemma. The decentralization reflected by $\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}$ is discussed in Section IV. Furthermore, the B_h and B_{tx}, which are constants here, are also examined in Section VII-A.

IV. DECENTRALIZATION INDICATED BY $H^\top PH$

We explore the potential of $\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}$ indicating decentralization. First, in Section IV-A, we discuss the essential conditions for a decentralization index in blockchain technology. Subsequently, in Section IV-B, assuming uniform block propagation time between all nodes, we theoretically establish that $\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}$ can indicate decentralization. Finally, in Section IV-C, we verify through simulation that $\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}$ retains its capactiy to indicate decentralization even under realistic network parameters for block propagation times between nodes.

A. CONDITIONS FOR A DECENTRALIZATION INDEX

We first explore the essential prerequisites for a decentralization index in blockchain and ascertain that $\boldsymbol{H}$ fulfills these conditions.

The definition of decentralization is ambiguous and can be viewed from various perspectives. We contend that the following two criteria are indispensable for a blockchain decentralization index (see Figure 3):

1) The degree of decentralization increases as the hash rate distribution becomes less concentrated. Conversely, decentralization decreases as the distribution of hash rates becomes more concentrated.
2) Decentralization positively correlates with the number of nodes present; thus, increasing the number of nodes

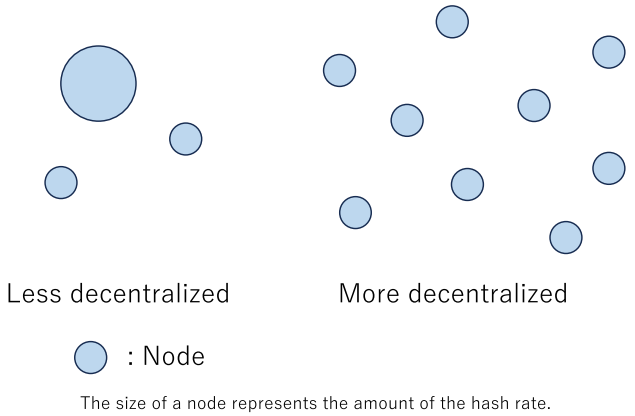


FIGURE 3. Decentralization conceptual diagram. The degree of decentralization increases with a greater number of nodes and less bias in each node's hash rate.

enhances decentralization. Conversely, a decrease in the number of nodes results in decreased decentralization.

In Proof of Work, a node's influence on block creation in the blockchain is determined by the proportion of its hash rate relative to the total hash rate. These two conditions for the decentralization index are designed to reflect the distribution of this influence. Considering both perspectives is crucial. For instance, even if many nodes possess small hash rates, if there is a significant gap in node hash rates, the enhancement in decentralization remains minimal.

Our delineated conditions for the decentralization index align with certain existing definitions of decentralization. For instance, in Buterin's article "The Meaning of Decentralization" [23], Buterin delineates decentralization into three axes and provides the following definitions.

1) Architectural Decentralization: How many physical computers is the system made of? How many of them can fail at any time without affecting the system?
2) Political Decentralization: How many individuals or organizations ultimately control the computers that the system is made up of?
3) Logical Decentralization: Does the system's interface and data structures appear as a single monolithic object or a formless swarm? A simple heuristic is whether cutting the system in half (including both providers and users) would allow both halves to continue operating independently as complete units.

For instance, architectural decentralization increases as the number of nodes grows and the distribution of hash rates becomes less concentrated. This aligns with Buterin's definition, which incorporates the number of nodes, and a less concentrated hash rate distribution implies that more nodes can fail without disrupting the blockchain. In practical terms, if a node with a substantial hash rate experiences a failure, it may cause a more noticeable temporary decline in transaction processing speed compared to the failure of a node with a smaller hash rate.

Similarly, political decentralization expands with more nodes and a less concentrated hash rate distribution. More nodes equate to more individuals or organizations controlling the blockchain, and the level of control each entity possesses depends on its proportion of the total hash rate.

It is important to note that from the standpoint of logical decentralization, the blockchain always remains centralized because it maintains a single state. Hence, this aspect of decentralization has not been explored in this study.

The vector $\boldsymbol{H}$, featured in the trilemma formula, denotes the distribution of hash rates, with the vector's length corresponding to the number of nodes. This correlation perfectly aligns with the two conditions outlined for the decentralization index.

B. THEORETICAL ANALYSIS OF $H^\top PH$

This section provides mathematical expressions to illustrate how the decentralization represented by $\boldsymbol{H}$ is manifested through $\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}$. Furthermore, we establish that $\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}$ encompasses the HHI, an established decentralization index.

$\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}$ is a quadratic form and can be expressed as follows:

$$\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H} = \sum_{i=1}^{n} \sum_{j=1, j\neq i}^{n} t_{ij} H_i H_j. \tag{16}$$

Here, the matrix $\boldsymbol{P}$ encompasses elements that are not directly related to decentralization. To simplify, let us consider a case where the block propagation time per byte, denoted as t_{ij}, remains identical for all nodes. In other words, each element of the matrix $\boldsymbol{P}$ is constant at a value of t_c. Leveraging $\sum_{i=1}^{n} H_i = 1$, we perform the following transformation:

$$\begin{aligned}
\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H} &= \sum_{i=1}^{n} \sum_{j=1, j\neq i}^{n} t_c H_i H_j \\
&= t_c \sum_{i=1}^{n} \sum_{j=1, j\neq i}^{n} H_i H_j \\
&= t_c \sum_{i=1}^{n} H_i \left(\sum_{j=1}^{n} H_j - H_i \right) \\
&= t_c \sum_{i=1}^{n} H_i \left(1 - H_i\right) \\
&= t_c \left(1 - \sum_{i=1}^{n} {H_i}^2 \right)
\end{aligned} \tag{17}$$

The maximum and minimum value of $\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}$ is as follows:

$$0 \leq \boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H} \leq t_c \left(1 - \frac{1}{n}\right). \tag{18}$$

Equation (17) exhibits an increase with decentralization, corresponding to a higher number of nodes and less biased hash rates. Conversely, Equation (17) demonstrates a decrease with decreasing decentralization, observed when the number of nodes decreases, and hash rates become more biased.

Moreover, the $\sum_{i=1}^{n} H_i^2$ component in Equation (17) corresponds to the existing decentralization index known as the HHI. A higher HHI indicates lower decentralization, while a lower HHI indicates higher decentralization. Equation (17) incorporates the expression for HHI expression and, owing to the negative sign, it inversely correlate with decentralization in the same form of HHI.

Thus, we have demonstarated that in scenarios where the block propagation time per byte t_{ij} is uniform across for all nodes, $\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}$ indirectly indicates decentralization through $\boldsymbol{H}$ and also encompasses HHI.

C. EXPERIMENTAL ANALYSIS OF $H^\top PH$ THROUGH SIMULATION

We verify through simulation that $\boldsymbol{H}$ indirectly shows decentralization through $\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}$, even when the block propagation time per byte, denoted as t_{ij}, is set to realistic values that vary among nodes.

The simulations are performed in two types:

- Fixing the number of nodes while varying the bias of the hash rate to evaluate $\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}$.
- Fixing the bias of the hash rate and varying the number of nodes to evaluate $\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}$. The hash rate bias is simulated for scenarios where nodes exhibit no bias and where a significant proportion of the hash rate is concentrated among top nodes.

SimBlock [34] serves as the simulation platform. All simulations are conducted up to a block height of 100000, employing the parameters outlined in Table 2 unless stated otherwise. Network parameters for Bitcoin in 2019, as computed by Nagayama et al. [35] are adopted. These parameters encompass node distribution, network latency, and bandwidth. The calculation methods for each parameter are as follows.

- Node distribution: Data from Bitnodes [36] was utilized to assess the number of nodes in each country. Because SimBlock categorizes nodes into six regions - North America, Europe, South America, Asia, Japan, and Australia - the distribution of nodes was computed for each region.
- Network latency: Representative cities from each country (including one city from the east and one from the west for the USA) were selected, and network latency data between these cities were sourced from WonderNetwork [37]. Inter-regional network latency was determined by calculating a weighted average of the network latencies, considering the number of nodes in each country.
- Bandwidth: Bandwidth data by country were referenced from testmy.net [38]. The bandwidth allocation for each region was determined using a weighted average that accounted for the number of nodes in each country.

1) VARIATION OF $H^\top PH$ WITH BIAS OF HASH RATE

Maintaining a fixed the number of nodes at 1000, the bias of the hash rate distribution is varied based on the Zipf distribution depicted in equation (19) ($s = 0, 0.5, 1.0, 1.5, 2.0$), and $\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}$ is evaluated. The Zipf distribution is characterized by the following equation:

$$f(k, s, N) = \frac{k^{-s}}{\sum_{n=1}^{N} n^{-s}}. \tag{19}$$

Here, s represents a parameter, N denotes the number of elements, and k signifies the rank when all elements are arranged in descending order. Notably, for $s = 1.0$, the k-th element's is $\frac{1}{k}$ of the value of the 1st element. For $s = 0$, all elements have the same value. The use of the Zipf distribution was to minimize arbitrariness when providing changes in the distribution of hash rates. As illustrated in Fig. 4, a smaller s value corresponds to a less biased distribution. The simulation results are summarized in Table 3 and Figure 5. For the reader's reference, table 3 also shows the proportion of hash rates of the top 5 nodes ($\boldsymbol{H_1}$–$\boldsymbol{H_5}$(%)) after arranging 1000 nodes in descending order of their hash rate ratios.

According to our two conditions for a decentralization index, a smaller the bias of the hash rate, the greater the decentralization, and the larger the bias of the hash rate, the smaller the decentralization. In Table 3, the smaller the value of s, the less biased the hash rate, indicating higher decentralization. It can be seen from Table 3 that in high decentralization situations ($s = 0$), $\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}$ is large, and in low decentralization situations ($s = 2.0$), $\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}$ is small. Moreover, Figure 5 shows that changes in bias within a range of large bias have a significant impact on the variation of $\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}$.

According to our two conditions for a decentralization index, a smaller bias in hash rate signifies greater decentralization, whereas a larger bias indicates reduced decentralization. In Table 3, a lower s value corresponds to a less biased hash rate distribution, indicating higher decentralization. It is evident from Table 3 that in scenarios with high decentralization ($s = 0$), $\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}$ exhibits a large value, whereas in situations with low decentralization ($s = 2.0$), $\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}$ is small. Additionally, Figure 5 shows that changes in bias within a range of significant bias levels profoundly influence the variation of $\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}$.

TABLE 2. Parameters for blockchain simulation.

Average block generation interval	600 s
Block size	2100080 byte
Degree distribution	Miller et al.'s [39] measurement results
Node distribution	Distribution of nodes in 6 regions
Network latency	Network latency between 6 regions
Bandwidth	Bandwidth in 6 regions

2) VARIATION OF $H^\top PH$ WITH THE NUMBER OF NODES

For hash rate distributions conforming to a Zipf distribution with $s = 0$ and 2.0, the number of nodes is varied (64, 128, 256, 512, 1024), and $\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}$ is assessed. The method of changing the number of nodes sets values as powers of two to ensure arbitrariness is minimized. The hash rate distributions for each case are summarized in Figs. 6 and 7. Additionally, The simulation results are summarized in Tables 4 and 5, and

TABLE 3. Values of $H^\top PH$ and decentralization indices based on the Zipf distribution parameter s. H_1–H_5 denote the proportion of hash rates held by the top 5 nodes relative to the entire network. A greater s value indicates a more biased the hash rate distribution.

s	0	0.5	1.0	1.5	2.0
$\boldsymbol{H^\top PH}$	$4.60 \cdot 10^{-6}$	$4.59 \cdot 10^{-6}$	$4.43 \cdot 10^{-6}$	$3.57 \cdot 10^{-6}$	$2.49 \cdot 10^{-6}$
Gini coefficient	0	0.318	0.734	0.953	0.992
HHI	$1.00 \cdot 10^{-3}$	$1.96 \cdot 10^{-3}$	$2.93 \cdot 10^{-2}$	0.185	0.400
Nakamoto coefficeint	501	262	24	2	1
For readers' reference:					
$\boldsymbol{H_1}(\%)$	0.10	1.62	13.36	39.23	60.83
$\boldsymbol{H_2}(\%)$	0.10	1.14	6.68	13.87	15.21
$\boldsymbol{H_3}(\%)$	0.10	0.93	4.45	7.55	6.76
$\boldsymbol{H_4}(\%)$	0.10	0.81	3.34	4.90	3.80
$\boldsymbol{H_5}(\%)$	0.10	0.72	2.67	3.51	2.43

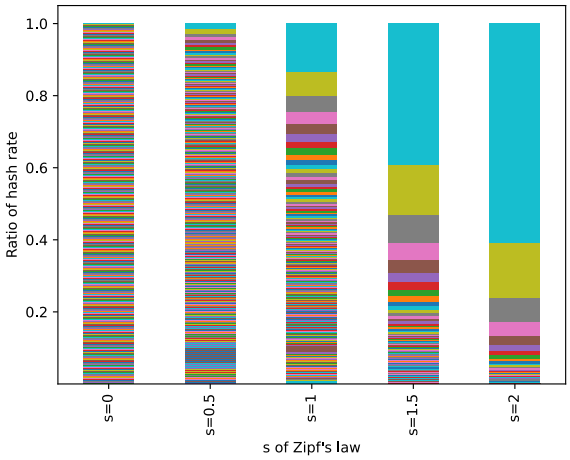


FIGURE 4. Distribution of hash rates among 1000 nodes following Zipf's law parameter s. A smaller the s, a less biased the distribution.

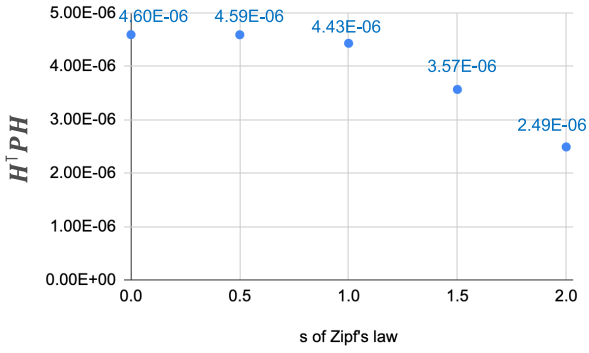


FIGURE 5. $H^\top PH$ based on the Zipf distribution parameter s.

Fig. 8. For the reader's reference, Tables 4 and 5 also show the proportion of hash rates of the top 5 nodes($\boldsymbol{H_1}$–$\boldsymbol{H_5}(\%)$) after arranging the nodes in descending order of their hash rate ratios.

In accordance with our two conditions for a decentralization index, higher decentralization is observed with a greater number of nodes, whereas lower decentralization is associated with fewer nodes. Table 4 portrays a scenario featuring no bias in the hash rate distribution ($s = 0$). As depicted in Table 4, in situations with a high number of nodes indicating high decentralization, $\boldsymbol{H^\top PH}$ exhibits

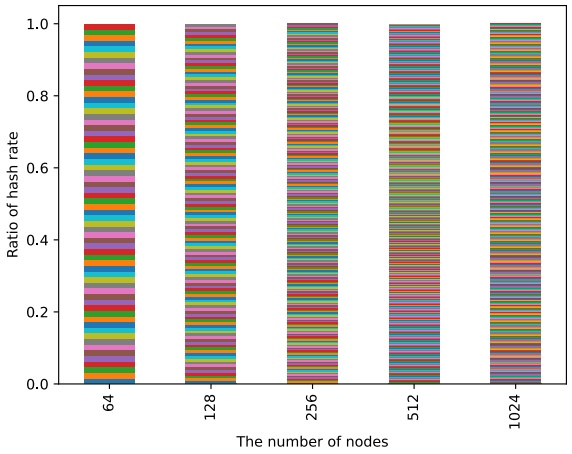


FIGURE 6. Distribution of hash rates corresponding to the number of nodes with Zipf distribution law parameter $s = 0$. In this scenario, where all nodes possess the same hash rate, the varying numbers of nodes represents the least biased situation.

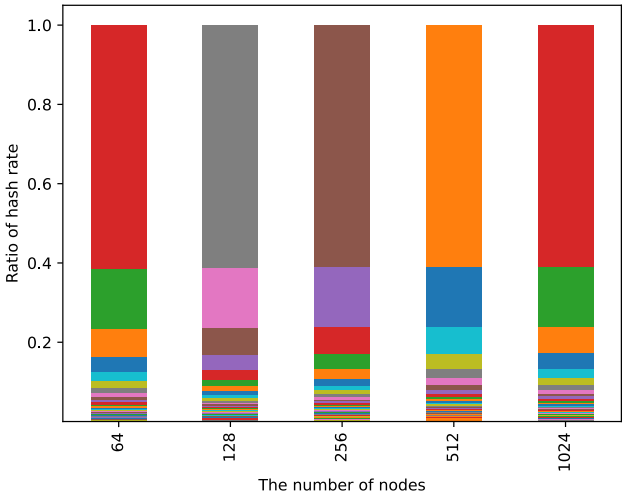


FIGURE 7. Distribution of hash rates based on the number of nodes with Zipf distribution law parameter $s = 2.0$. Nodes with larger hash rates dominate the majority of the hash rate, and increasing the number of nodes only adds more nodes with smaller hash rates.

larger values, whereas in situations where the number of nodes is low, indicative of low decentralization, $\boldsymbol{H^\top PH}$ tends to be smaller. Additionally, Fig. 8 illustrates that changes in the number of nodes within a range of a small number of nodes significantly influence the fluctuation of $\boldsymbol{H^\top PH}$.

TABLE 4. Values of $H^\top PH$ and decentralization indices corresponding to the number of nodes when $s = 0$. The value $s = 0$ signifies a state with the least bias in hash rate distribution.

Number of nodes	64	128	256	512	1024
$\boldsymbol{H^\top PH}$	$3.13 \cdot 10^{-6}$	$3.46 \cdot 10^{-6}$	$3.83 \cdot 10^{-6}$	$4.21 \cdot 10^{-6}$	$4.61 \cdot 10^{-6}$
Gini coefficient	0	0	0	0	0
HHI	$1.56 \cdot 10^{-2}$	$7.81 \cdot 10^{-3}$	$3.91 \cdot 10^{-3}$	$1.95 \cdot 10^{-3}$	$9.77 \cdot 10^{-4}$
Nakamoto coefficient	33	65	129	257	513
For readers' reference:					
$\boldsymbol{H_1}(\%)$	1.56	0.781	0.391	0.195	$9.77 \cdot 10^{-2}$
$\boldsymbol{H_2}(\%)$	1.56	0.781	0.391	0.195	$9.77 \cdot 10^{-2}$
$\boldsymbol{H_3}(\%)$	1.56	0.781	0.391	0.195	$9.77 \cdot 10^{-2}$
$\boldsymbol{H_4}(\%)$	1.56	0.781	0.391	0.195	$9.77 \cdot 10^{-2}$
$\boldsymbol{H_5}(\%)$	1.56	0.781	0.391	0.195	$9.77 \cdot 10^{-2}$

TABLE 5. Values of $H^\top PH$ and decentralization indices corresponding to the number of nodes when $s = 2.0$. The value $s = 2.0$ signifies a state where a few top nodes occupy most of the network's hash rate.

Number of nodes	64	128	256	512	1024
$\boldsymbol{H^\top PH}$	$2.09 \cdot 10^{-6}$	$2.58 \cdot 10^{-6}$	$2.78 \cdot 10^{-6}$	$2.52 \cdot 10^{-6}$	$2.80 \cdot 10^{-6}$
Gini coefficient	0.925	0.956	0.975	0.986	0.992
HHI	0.408	0.404	0.402	0.401	0.400
Nakamoto coefficient	1	1	1	1	1
For readers' reference:					
$\boldsymbol{H_1}(\%)$	61.37	61.08	60.93	60.87	60.83
$\boldsymbol{H_2}(\%)$	15.34	15.27	15.23	15.21	15.21
$\boldsymbol{H_3}(\%)$	6.82	6.79	6.77	6.76	6.76
$\boldsymbol{H_4}(\%)$	3.84	3.82	3.81	3.80	3.80
$\boldsymbol{H_5}(\%)$	2.45	2.44	2.44	2.43	2.43

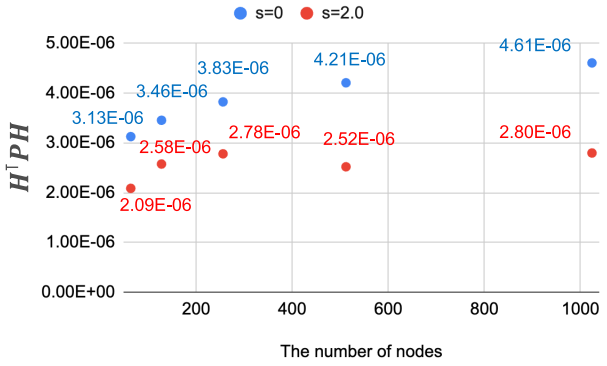


FIGURE 8. Variation of $H^\top PH$ according to the number of nodes.

Table 5 illustrates a scenario with a Zipf distribution of $s = 2.0$, where the hash rate of a few top nodes occupies a large portion of the total hash rate. It is evident from Table 5 that in situations with a high number of nodes indicating high decentralization, $\boldsymbol{H^\top PH}$ tends to be larger. In conrast, in situations with a low number of nodes indicating low decentralization, $\boldsymbol{H^\top PH}$ tend to be smaller. However, unlike the case with $s = 0$, increasing the number of nodes with a small hash rate in a scenario with a large bias in hash rate does not contribute as significantly to the improvement of decentralization. Furthermore, the impact of bandwidth and latency in the region where nodes with a large hash rate are allocated becomes significant, indicating that $\boldsymbol{H^\top PH}$ does not consistently fluctuate with the level of decentralization. Moreover, Figure 8 highlights that changes in the number of nodes within a range of a small number of nodes have a notable impact on the fluctuation of $\boldsymbol{H^\top PH}$.

In Sections IV-B and IV-C, the block propagation time among nodes was either fixed to identical or realistic, implying that $\boldsymbol{P}$ was treated as constant. The variation of this constant $\boldsymbol{P}$ is explored in Section VII-B.

V. REVIEW OF EXISTING DECENTRALIZATION INDICES

Several decentralization indices exist, yet studies have inadequately addressed the definition of decentralization and the adequacy of these indices. Consequently, it remains uncertain which decentralization index best correlates with the decentralization aspect of the trilemma. This section evaluates the validity of current decentralization indices according to the two conditions outlined in IV-A. Additionally, we elucidate the relationship between $\boldsymbol{H^\top PH}$ and established decentralization indices.

In Section V-A, we introduce the existing decentralization indices. Then, in Section V-B, we analyze these indices (Gini coefficient, HHI, and Nakamoto coefficient) based on the two conditions outlined in Section IV-A. Our analysis identifies HHI as the most suitable index according to these conditions. Additionally, we compute correlation coefficients between the existing decentralization indices and $\boldsymbol{H^\top PH}$. The findings reveal that the correlation between $\boldsymbol{H^\top PH}$ and HHI is the strongest, suggesting that $\boldsymbol{H^\top PH}$ reflects decentralization similarly to HHI.

A. EXISTING DECENTRALIZATION INDICES

1) GINI COEFFICIENT

The Gini coefficient [40] is a common metric for evaluating income inequality in economics. A higher Gini coefficient indicates greater inequality, whereas a lower coefficient

indicates greater equality. This index is also applied to gauge decentralization levels in blockchain, suggesting that a lower Gini coefficient indicates a more evenly distributed system, implying a higher degree of decentralization. Conversely, a higher Gini coefficient suggests a more concentrated system, hinting at potential risks of centralization. The Gini coefficient $G[\boldsymbol{H}]$ can be expressed using the elements of $\boldsymbol{H}$ as follows:

$$G[\boldsymbol{H}] = \frac{\sum_{i=1}^{n}\sum_{j=1}^{n}|H_i - H_j|}{2n^2 \cdot \mathrm{Avg}[\boldsymbol{H}]} = \frac{\sum_{i=1}^{n}\sum_{j=1}^{n}|H_i - H_j|}{2n}, \tag{20}$$

where $\mathrm{Avg}[\boldsymbol{H}]$ is the average of $\boldsymbol{H}$'s elements. Furthermore, the maximum and minimum values of $G[\boldsymbol{H}]$ can be expressed as:

$$0 \leq G[\boldsymbol{H}] \leq 1 \tag{21}$$

2) HERFINDAHL-HIRSCHMAN INDEX (HHI)

The HHI measures market concentration, considering the market share held by each company within a particular industry, represented by the sum of the squares of each companies' share. A higher HHI indicates more concentration, while a lower HHI suggests more distribution. This index is also applied as a measure of decentralization in blockchain system, implying that a lower HHI suggests a higher degree of decentralization. Conversely, a higher HHI implies at potential risks of centralization. Using the elements of vector $\boldsymbol{H}$, HHI can be expressed as:

$$\mathrm{HHI}[\boldsymbol{H}] = \sum_{i=1}^{n} H_i^2. \tag{22}$$

Moreover, the maximum and minimum values of $\mathrm{HHI}[\boldsymbol{H}]$ can be expressed as follows:

$$\frac{1}{n} \leq \mathrm{HHI}[\boldsymbol{H}] \leq 1. \tag{23}$$

3) NAKAMOTO COEFFICIENT

The Nakamoto coefficient [41] is a key index for assessing decentralization, defined as the minimum number of nodes necessary to control over 50% of the total network's hash rate. Essentially, it indicates the minimum difficulty of a 51% attack. Intuitively, a higher Nakamoto coefficient suggests a higher degree of decentralization, whereas a lower coefficient indicates potential centralization risks. The Nakamoto coefficient $\mathrm{N}[\boldsymbol{H}]$ can be expressed as follows:

$$\mathrm{N}[\boldsymbol{H}] = \min\{k \in [1, \ldots, n] : \sum_{i=1}^{k} H_i > 0.5\}. \tag{24}$$

Furthermore, the maximum and minimum values of $\mathrm{N}[\boldsymbol{H}]$ can be expressed as follows:

$$1 \leq \mathrm{N}[\boldsymbol{H}] \leq \frac{n+1}{2}. \tag{25}$$

B. CONFORMANCE TO THE TWO CONDITIONS FOR DECENTRALIZATION INDICES

To ascertain whether the current decentralization indices adhere to the two conditions for a decentralization index, we compute the Gini coefficient, HHI, and Nakamoto coefficient while varying the number of nodes and the distribution of hash rates. The computations and subsequent analysis determined that the HHI is most suitable for our two conditions for a decentralization index among these indices.

1) CHANGES IN DECENTRALIZATION DEPENDING ON HASH RATE DISTRIBUTION BIAS

We maintain the number of nodes at 1000 and adjust the bias in hash rate distribution based on the Zipf distribution (19) with s values of 0, 0.5, 1.0, 1.5, 2.0. As depicted in Fig. 4, a smaller s value corresponds to a distribution with less bias. The computed results are summarized in Table 3. For the reader's reference, table 3 also shows the proportion of hash rates of the top 5 nodes ($\boldsymbol{H_1}$–$\boldsymbol{H_5}$(%)) after arranging 1000 nodes in descending order of their hash rate ratios.

In accordance with the two conditions for a decentralization index, a smaller bias in hash rate indicates higher decentralization, while a larger bias signifies lower decentralization. In Table 3, smaller s values lead to less hash rate bias, indicative of higher decentralization. The table reveal that the Nakamoto coefficient is high in scenarios with high decentralization ($s = 0$), whereas the Gini coefficient and HHI are low. Conversely, the Nakamoto coefficient is low in situations with low decentralization ($s = 2.0$), while the Gini coefficient and HHI are high. This suggest that all indices effectively capture decentralization in line with the two conditions for a decentralization index.

2) CHANGES IN DECENTRALIZATION DEPENDING ON THE NUMBER OF NODES

The distribution of hash rates is computed for Zipf distributions with $s = 0$ and 2.0, varying the number of nodes to 64, 128, 256, 512, 1024. Subsequently we calculate the Gini coefficient, HHI, and Nakamoto coefficient. The distribution of hash rates for each case is illustrated in Figures 6 and 7. The computed results are summarized in Table 4 and Table 5. For the reader's reference, Table 4 and Table 5 also show the proportion of hash rates of the top 5 nodes ($\boldsymbol{H_1}$–$\boldsymbol{H_5}$(%)) after arranging the nodes in descending order of their hash rate ratios.

Table 4 illustrates a scenario with a Zipf distribution of $s = 0$, representing an evenly distributed hash rate. According to our two conditions for a decentralization index, a greater number of nodes correspond to higher decentralization, while a smaller number of nodes indicates lower decentralization. In instances of high decentralization owing to a larger number of nodes, the HHI is lower, and the Nakamoto coefficient is higher. Conversely, in situations of low decentralization owing to a smaller number of nodes, the HHI is higher, and the Nakamoto coefficient is lower. However, the Gini coefficient

remains 0 regardless of the number of nodes, failing to meet the two conditions for our decentralization index.

Table 5 portrays a scenario with a Zipf distribution of $s = 2.0$, where the hash rates of a few top nodes occupy a significant portion of the total hash rate. According to our two conditions for a decentralization index, a larger number of nodes leads to higher decentralization, while fewer nodes result in lower decentralization. In case of higher decentralization owing to more nodes, the HHI is lower. Conversely, in case of lower decentralization due to fewer nodes, the HHI is higher. The Gini coefficient is smaller in situations with lower decentralization and larger in situations with higher decentralization, thus not serving as a reliable index for decentralization. Furthermore, the Nakamoto coefficient consistently remains at a value of 1, failing to meet the two conditions for a decentralization index.

Therefore, among the decentralization indices considered, the HHI most effectively satisfies the two conditions.

3) DISCUSSION ON CONFORMANCE

In Section V-B2, when $s = 0$, the Gini coefficient does not meet our two conditions for a decentralization index. Likewise, when $s = 2.0$, the Gini and Nakamoto coefficients fail to meet these conditions. Let us analyze the underlying causes.

Regarding the behavior of the Gini coefficient when $s = 0$ in Section V-B2, we conduct a generalized analysis using the vector $\boldsymbol{H_a}$ representing the extreme situation as follows:

$$\boldsymbol{H_a} = \begin{pmatrix} \frac{1}{k} \\ \frac{1}{k} \\ \vdots \\ \frac{1}{k} \end{pmatrix}. \tag{26}$$

$\boldsymbol{H_a}$ is a vector containing k elements of $\frac{1}{k}$. For simplicity, we assume each node has the same hash rate. In such a scenario, a decentralization index should reflect higher decentralization with a larger number of nodes k, as each node's influence on the total becomes smaller. However, computing the Gini coefficient for $\boldsymbol{H_a}$ results in 0, regardless of the node count k. On the other hand, the HHI of $\boldsymbol{H_a}$ is $\frac{1}{k}$, effectively indicating higher decentralization with increasing k. This disparity arises because the Gini coefficient formula, which accounts for the differences between elements, invariably results in 0 when each node has the same hash rate, irrespective of the number of nodes. In contrast, the HHI formula, which squares each element and then sums them, effectively reflects the impact of node count because the square of each element becomes smaller as the node count increases.

Now, let us analyze the behavior of the Gini coefficient when $s = 2.0$ in Section V-B2, by considering a generalized scenario represented by the vector $\boldsymbol{H_b}$:

$$\boldsymbol{H_b} = \begin{pmatrix} 0.5 \\ 0.3 \\ 0.2 \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{27}$$

$\boldsymbol{H_b}$ is a vector with elements 0.5, 0.3, 0.2, and 0 for i elements, totaling $i + 3$ elements. This distribution indicates that the top 3 nodes dominate the hash rate, while the remaining lower-ranked nodes have negligible hash rate. For simplicity, lower nodes are assigned a hash rate of 0. When evaluating the decentralization of $\boldsymbol{H_b}$, the decentralization indices should remain consistent regardless of i. This is because adding nodes with negligible hash rates does not significantly affect each node's influence on the total hash rate, thus not contributing much to decentralization. However, calculating the Gini coefficient for $\boldsymbol{H_b}$ results in $\frac{i+0.6}{i+3}$, indicating an increase in the Gini coefficient (implying reduced decentralization) as i increases. Conversely, the HHI for $\boldsymbol{H_b}$ remains constant at 0.38, regardless of i. This occurs because the Gini coefficient formula, which sums the differences between elements, overestimates the impact of lower nodes. In contrast, the HHI formula evaluates individual elements by squaring them, thereby reducing the impact of nodes with small hash rates in the sum.

Next, let us analyze the behavior of the Nakamoto coefficient when $s = 2.0$ in Section V-B2, using a generalized scenario represented by the vector $\boldsymbol{H_c}$:

$$\boldsymbol{H_c} = \begin{pmatrix} 0.31 \\ 0.2 \\ \frac{0.49}{j} \\ \vdots \\ \frac{0.49}{j} \end{pmatrix}. \tag{28}$$

$\boldsymbol{H_c}$ is a vector comprising elements 0.31, 0.2, and j elements of $\frac{0.49}{j}$, totaling $j + 2$ elements, where j is an integer greater than 3. With increasing j, the influence of each of the j nodes on the total hash rate should theoretically decrease, suggesting lower decentralization. However, the Nakamoto coefficient for $\boldsymbol{H_c}$ remains constant at 2 regardless of j. This occurs because the Nakamoto coefficient solely indicates the minimum coalition difficulty and does not consider the distribution of lower hash rates among nodes.

C. CORRELATION BETWEEN EXISTING DECENTRALIZATION INDICES AND $H^\top PH$

Using Pearson correlation coefficient, we analyze the correlation between existing decentralization indices and $\boldsymbol{H}^\top \boldsymbol{PH}$, as listed in Table 6. It is essential to understand that the aim behind each index and $\boldsymbol{H}^\top \boldsymbol{PH}$ is that with higher decentralization, the Gini coefficient and HHI should decrease, while the Nakamoto coefficient and $\boldsymbol{H}^\top \boldsymbol{PH}$ should

increase. In other words, a Gini coefficient and HHI closer to -1, and a Nakamoto coefficient closer to 1, indicate a level of decentralization similar to that shown by $\boldsymbol{H}^\top \boldsymbol{PH}$.

The first row of Table 6 shows the correlation between existing decentralization indices and $\boldsymbol{H}^\top \boldsymbol{PH}$ when the hash rate bias is varied. It is evident that HHI has the strongest correlation with $\boldsymbol{H}^\top \boldsymbol{PH}$.

Moving to the second row of Table 6, we examine the correlation in the context of a Zipf distribution with $s = 0$ (where all nodes have the same hash rate) and varying the number of nodes. HHI and the Nakamoto coefficient demonstrate a strong correlation with $\boldsymbol{H}^\top \boldsymbol{PH}$. As noted in Section V-B2, the Gini coefficient consistently results in 0, rendering its variance 0 and making it impossible to calculate a correlation coefficient.

The third row of Table 6 addresses a Zipf distribution with $s = 2.0$ and varying the number of nodes. In this case, HHI and the Gini coefficient strongly correlate with $\boldsymbol{H}^\top \boldsymbol{PH}$. However, as previously discussed in Section V-B2, the Gini coefficient fails to represent the level of decentralization adequately, and its correlation coefficient shows a positive correlation, which is inappropriate. Moreover, as stated in Section V-B2, the Nakamoto coefficient maintains the same value for all cases, resulting in a variance of 0 and making it impossible to calculate a correlation coefficient.

From the above, the decentralization represented through $\boldsymbol{H}^\top \boldsymbol{PH}$ is similar to the form of the HHI.

VI. VERIFICATION OF THE TRILEMMA THROUGH SIMULATION

This section aims to validate the trilemma formula, denoted as (15), through simulation experiments.

The fork rate F, indicative of security, is indirectly assessed by configuring parameters related to the scalability (n_{tx} and T) and decentralization (n and s). Accordingly, we conduct simulations based on the following two patterns:

- By keeping the decentralization parameter constant and varying the scalability parameter, we can gauge the fork rate and verify the trilemma formula's accuracy.
- By maintaining the scalability parameter constant and varying the decentralization parameter, we can measure the fork rate and assess the trilemma formula's validity.

Specifically, we perform the following four simulations:

1) With the decentralization parameter and the average block generation time T, which is a scalability parameter, fixed, we vary the number of transactions per block n_{tx}, which is the other scalability parameter, to measure the fork rate. We then verify whether the product of the three terms in the trilemma formula is close to 1. We adjust n_{tx} to 2100, 3150, 4200, 5250, 6300. The parameters T is set to 600 s. $\boldsymbol{H}$ represents the number of nodes at 1000, based on Zipf distribution with $s = 1.0$. The distribution of hash rates is shown in Fig. 9.
2) With the decentralization parameter and the number of transactions per block n_{tx}, which is a scalability parameter, fixed, we vary the average block generation time T, which is the other scalability parameter, to measure the fork rate. We then verify whether the product of the three terms in the trilemma formula is close to 1. We change T to 300, 450, 600, 750, 900 s. The number of transactions n_{tx} is 4200. $\boldsymbol{H}$ represents 1000 nodes arranged according to Zipf distribution with $s = 1.0$. The hash rate distribution is depicted in Fig. 9.
3) With the scalability parameter and the number of nodes in $\boldsymbol{H}$, which is a decentralization parameter, fixed, we vary the hash rate distribution of $\boldsymbol{H}$, which is the other decentralization parameter, to measure the fork rate. We then verify whether the product of the three terms in the trilemma formula is close to 1. We change the hash rate distribution of $\boldsymbol{H}$ according to Zipf distribution with $s = 0, 0.5, 1.0, 1.5, 2.0$. The number of nodes is set to 1000, T to 600 s, and n_{tx} to 4200. The hash rate distribution is shown in Fig. 10.
4) With the scalability parameter and the hash rate distribution of $\boldsymbol{H}$, which is a decentralization parameter, fixed, we vary the number of nodes in $\boldsymbol{H}$, the other decentralization parameter, to measure the fork rate. We then verify whether the product of the three terms in the trilemma formula is close to 1. The number of nodes in $\boldsymbol{H}$ changes to 64, 128, 256, 512, 1024, following Zipf distribution with $s = 0$. T is set to 600 s, and n_{tx} to 4200. The hash rate distribution is shown in Fig. 11.

Simblock [34] was utilized for simulations. Network parameters for Bitcoin in 2019, as computed by Nagayama et al. [35] are adopted as with the simulation in Section IV-C. All simulations were conducted up to a height of 100000 blocks, with the actual block header size B_h being 80 bytes and the transaction size B_{tx}, based on recent Bitcoin data [42], being 500 bytes. We run the simulation up to 100000 blocks because Sakurai and Shudo [33] shows that approximately 100,000 blocks are required for the fork rate to converge. The standard of the number of transaction n_{tx} and the average block generation time T is set 4200 and 600s respectively, following Bitcoin (Bicoin TPS is commonly 7 TPS). The use of the Zipf distribution was to minimize arbitrariness when providing changes in the distribution of hash rates. The parameters not mentioned are the same as in Table 2. The results of the simulations are summarized in Tables 7 - 10 and Figs. 12 - 15.

In all simulations, the product of the three terms of the trilemma formula was found to be close to 1. Since the product of the three terms equals about 1, it can be seen that the trilemma formula holds true in this simulator. From the simulation result, the following has been demonstrated: in situations where the decentralization parameter is fixed, an increase in the scalability parameter leads to an increase in the fork rate (a decrease in security). The opposite is also true. Additionally, when the scalability parameter is fixed and the decentralization parameter increases, the fork rate increases (security decreases). The opposite is also true.

TABLE 6. Comparison of correlation coefficients between $H^\top PH$ and each index.

	Gini	HHI	Nakamoto
Correlation coefficient with s (1000 nodes)	-0.773	-0.9996	0.635
Correlation coefficient with the number of nodes ($s = 0$)	\	-0.920	0.945
Correlation coefficient with the number of nodes ($s = 2.0$)	0.857	-0.753	\

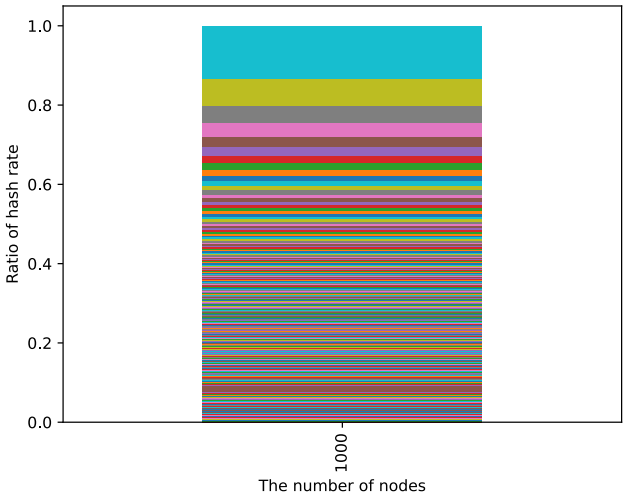


FIGURE 9. Hash rate distribution set in simulations when varying the number of transactions n_{tx} per block and the block generation interval T.

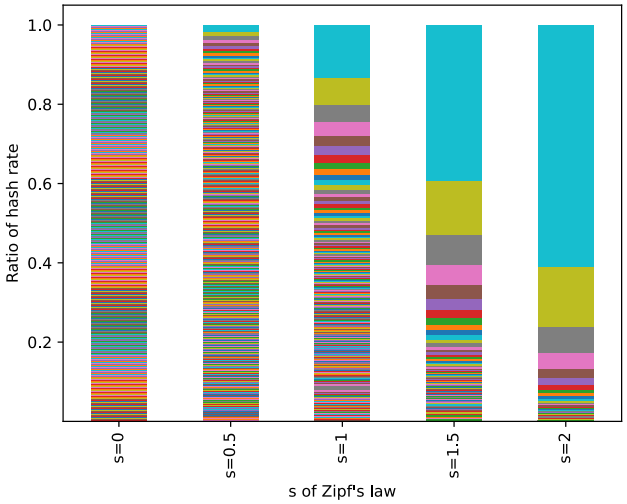


FIGURE 10. Hash rate distribution corresponding to the zipf distribution parameter s. The smaller the s, the less biased the distribution.

VII. TWO APPROACHES TO IMPROVE TRILEMMA PROPERTIES UNDER THE CONSTRAINTS OF THE TRILEMMA

We explore strategies to enhance blockchain trilemma properties within the constraints of the trilemma from our trilemma formula. Existing methods that improve trilemma properties while adhering to the trilemma's constraints can be categorized into two types: those focusing on "reduce B_h and B_{tx}", and those targeting "optimize the elements within $\boldsymbol{P}$".

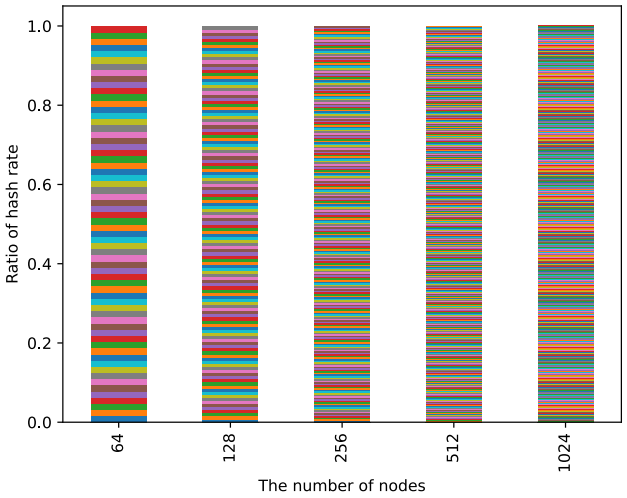


FIGURE 11. Hash rate distribution corresponding to the number of nodes.

A. APPROACHES TO REDUCE B_h AND B_{tx}

In Section II-C, we first addressed the trilemma in equation (15) by assuming B_h and B_{tx} to be constant. However, we now deviate from this assumption of constancy for B_h and B_{tx} and seek to minimize them in (15).

When we decerease the values of B_h and B_{tx}, in (15),this has no adversary impact on $\frac{n_{tx}}{T}$, $\frac{1}{F}$, or the distribution of $\boldsymbol{H}$. Consequently, the decrease in B_h and B_{tx} can be allocated to improvements in scalability, security, or decentralization. This approach aims to enhance blockchain's trilemma properties while abiding by the constraints of the trilemma. It is important to clarify that "the block size" does not denote the size of blocks included in the main chain, but the size of the data(i.e. sketch of Compact Block Relay [43]) when they are propagated for consensus. For instance, technologies such as Bitcoin's Compact Block Relay [43], Graphene [19], and the optimization of block generation notifications in the blockchain using bloom filters [44] are instrumental in improving trilemma properties through the reduction of B_h and B_{tx}. Moreover, the technique observed in Fruitchains [45] and Prism [28], which entails propagating blocks containing multiple transactions not meeting the target in advance and specifying these blocks in other blocks to reduce the size of data needed for consensus, can also be considered as one of the methods to reduce B_h and B_{tx}. This approach helps in specifying numerous transactions while aiming to minimize the data footprint for achieving consensus. These method reach its scalability limit because of the constraints imposed by the trilemma, but rather due to physical limitations such as bandwidth [28].

TABLE 7. Product of the three terms corresponding to the number of transactions n_{tx} in a block.

n_{tx}	2100	3150	4200	5250	6300
$\frac{n_{tx}}{T}$	3.50	5.25	7.00	8.75	10.5
F	$7.71 \cdot 10^{-3}$	$1.19 \cdot 10^{-2}$	$1.54 \cdot 10^{-2}$	$1.85 \cdot 10^{-2}$	$2.17 \cdot 10^{-2}$
$\frac{B_h+B_{tx} \cdot n_{tx}}{T}$	$7.00 \cdot 10^{3}$	$4.67 \cdot 10^{3}$	$3.50 \cdot 10^{3}$	$2.80 \cdot 10^{3}$	$2.33 \cdot 10^{3}$
$\frac{1}{F}$	130	84.0	64.8	54.2	46.0
$\boldsymbol{H}^\top \boldsymbol{P} \boldsymbol{H}$	$4.67 \cdot 10^{-6}$	$4.51 \cdot 10^{-6}$	$4.43 \cdot 10^{-6}$	$4.38 \cdot 10^{-6}$	$4.36 \cdot 10^{-6}$
Product of the three terms	1.06	0.99	1.01	1.04	1.05

TABLE 8. Product of the three terms according to the block generation interval T.

T	300	450	600	750	900
$\frac{n_{tx}}{T}$	14.0	9.33	7.00	5.60	4.67
F	$3.00 \cdot 10^{-2}$	$2.00 \cdot 10^{-2}$	$1.54 \cdot 10^{-2}$	$1.26 \cdot 10^{-2}$	$1.00 \cdot 10^{-3}$
$\frac{B_h+B_{tx} \cdot n_{tx}}{T}$	$7.00 \cdot 10^{3}$	$4.67 \cdot 10^{3}$	$3.50 \cdot 10^{3}$	$2.80 \cdot 10^{3}$	$2.33 \cdot 10^{3}$
$\frac{1}{F}$	33.3	49.9	64.8	79.7	99.8
$\boldsymbol{H}^\top \boldsymbol{P} \boldsymbol{H}$	$4.43 \cdot 10^{-6}$	$4.44 \cdot 10^{-6}$	$4.43 \cdot 10^{-6}$	$4.43 \cdot 10^{-6}$	$4.43 \cdot 10^{-6}$
Product of the three terms	1.03	1.03	1.01	0.99	1.03

TABLE 9. Product of the three terms corresponding to the zipf distribution parameter s. The smaller the s, the less skewed the distribution.

s	0	0.5	1.0	1.5	2.0
$\boldsymbol{H_1}$ (%)	0.10	1.62	13.36	39.23	60.83
$\boldsymbol{H_2}$ (%)	0.10	1.14	6.68	13.87	15.21
$\boldsymbol{H_3}$ (%)	0.10	0.93	4.45	7.55	6.76
$\boldsymbol{H_4}$ (%)	0.10	0.81	3.34	4.90	3.80
$\boldsymbol{H_5}$ (%)	0.10	0.72	2.67	3.51	2.43
F	$1.57 \cdot 10^{-2}$	$1.61 \cdot 10^{-2}$	$1.54 \cdot 10^{-2}$	$1.25 \cdot 10^{-2}$	$8.61 \cdot 10^{-3}$
$\frac{B_h+B_{tx} \cdot n_{tx}}{T}$	$3.50 \cdot 10^{3}$	$3.50 \cdot 10^{3}$	$3.50 \cdot 10^{3}$	$3.50 \cdot 10^{3}$	$3.50 \cdot 10^{3}$
$\frac{1}{F}$	63.6	62.2	64.8	79.9	116
$\boldsymbol{H}^\top \boldsymbol{P} \boldsymbol{H}$	$4.60 \cdot 10^{-6}$	$4.59 \cdot 10^{-6}$	$4.43 \cdot 10^{-6}$	$3.57 \cdot 10^{-6}$	$2.49 \cdot 10^{-6}$
Product of the three terms	1.02	1.00	1.01	1.00	1.01

TABLE 10. Product of the three terms corresponding to the number of nodes.

Number of nodes	64	128	256	512	1024
$\boldsymbol{H_1}$ (%)	1.56	0.781	0.391	0.195	$9.77 \cdot 10^{-2}$
$\boldsymbol{H_2}$ (%)	1.56	0.781	0.391	0.195	$9.77 \cdot 10^{-2}$
$\boldsymbol{H_3}$ (%)	1.56	0.781	0.391	0.195	$9.77 \cdot 10^{-2}$
$\boldsymbol{H_4}$ (%)	1.56	0.781	0.391	0.195	$9.77 \cdot 10^{-2}$
$\boldsymbol{H_5}$ (%)	1.56	0.781	0.391	0.195	$9.77 \cdot 10^{-2}$
F	$1.06 \cdot 10^{-2}$	$1.19 \cdot 10^{-2}$	$1.41 \cdot 10^{-2}$	$1.45 \cdot 10^{-2}$	$1.57 \cdot 10^{-2}$
$\frac{B_h+B_{tx} \cdot n_{tx}}{T}$	$3.50 \cdot 10^{3}$	$3.50 \cdot 10^{3}$	$3.50 \cdot 10^{3}$	$3.50 \cdot 10^{3}$	$3.50 \cdot 10^{3}$
$\frac{1}{F}$	94.2	83.7	70.8	69.1	63.7
$\boldsymbol{H}^\top \boldsymbol{P} \boldsymbol{H}$	$3.13 \cdot 10^{-6}$	$3.46 \cdot 10^{-6}$	$3.83 \cdot 10^{-6}$	$4.21 \cdot 10^{-6}$	$4.61 \cdot 10^{-6}$
Product of the three terms	1.03	1.01	0.95	1.02	1.03

B. OPTIMIZATION OF ELEMENTS WITHIN P

In this section, we discuss the approaches to improve the trilemma properties of the blockchain by reducing the elements of $\boldsymbol{P}$.

Focusing on (16), by decreasing the value of each element in $\boldsymbol{P}$, we can reduce $\boldsymbol{H}^\top \boldsymbol{P} \boldsymbol{H}$. This is equivalent to enhancing the bandwidth, reducing latency, and shortening block verification time. It does not affect the elements that represent decentralization, which is $\boldsymbol{H}$. In addition, it does not decrease $\frac{n_{tx}}{T}$ or $\frac{1}{F}$. Therefore, the reduction in each element inside $\boldsymbol{P}$ can be allocated to increase scalability, security, or decentralization. This is an approach to improve trilemma properties within the constraints of the trilemma. For instance, in the selection of neighboring nodes [46], the trilemma properties of the blockchain is improved by prioritizing the selection of nodes with fast block propagation. Technological innovations can enhance communication performance, which in turn improves the trilemma properties, even within the constraints of the trilemma. Moreover, in Bitcoin's Compact Block Relay [43], the security of the blockchain is improved by sending sketches to related nodes before block verification is complete.

Revisiting Equation (16), especially between nodes where the product of two hash rates is large, improving

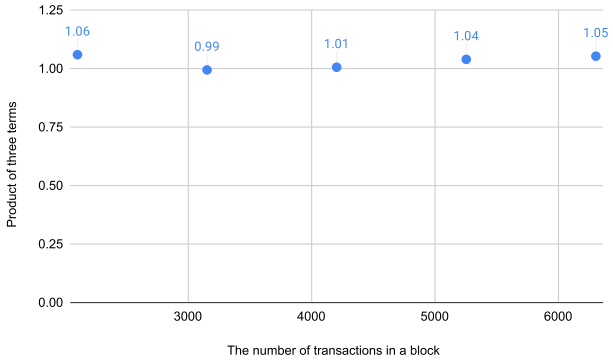


FIGURE 12. Product of the three terms corresponding to the number of transactions n_{tx} in a block.

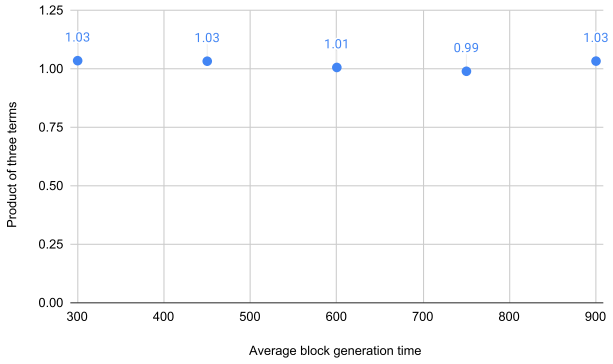


FIGURE 13. Product of the three terms corresponding to the block generation interval T.

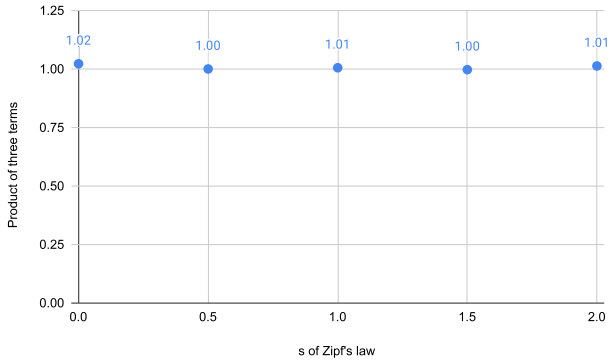


FIGURE 14. Product of the three terms corresponding to the zipf distribution parameter s. The smaller the s, the less biased the distribution.

communication performance can more efficiently reduce $\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}$ than improving the communication performance between other nodes. In other words, each node should allocate its network resources to increase bandwidth and reduce latency towards nodes with larger hash rates. This is equivalent to speeding up communication between nodes operated by mining pools.

In Section IV-B and IV-C, we assume that the block propagation time between each node is equal. If the block propagation time diverge among nodes, as demonstrated in this chapter, $\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}$, which indirectly indicates the

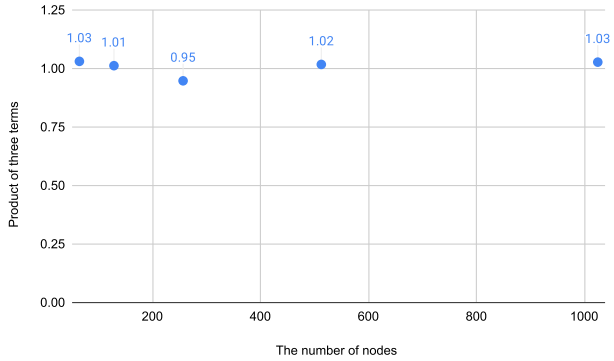


FIGURE 15. Product of the three terms corresponding to the number of nodes.

decentralization of H, increase or decrease depending on the block propagation time between each node.

VIII. DISCUSSION AND OPEN PROBLEMS

In this section, we document the discussion and the open problems of the trilemma formula.

A. COMPARISON WITH BUTERIN'S TRILEMMA

Here, we compare the three properties of Buterin's trilemma with the three properties of our trilemma formula, pointing out the similarities, differences, and the aspects in which our properties are more appropriate.

1) SCALABILITY

Buterin defines scalability as "whether the total number of transactions the system can handle exceeds the number of transactions each node can process." On the other hand, our mathematical definition of scalability specifies TPS, making it clear how many transactions can be processed. Although both of them focus on what extent the system can process transactions, our definition of scalability is more rigorous. Furthermore, when measuring a chain's scalability, TPS is often used as shown by [12]. It is a standard and reasonable measure of scalability.

2) DECENTRALIZATION

In Buterin's article on the trilemma [8], decentralization is defined as "the system being able to run in a scenario where each participant only has access to $O(c)$ resources." In our formula, decentralization represents the number of nodes and hash rate distribution. Although the definitions of decentralization by Buterin and us seem entirely different, they are related. First, we reinterpret Buterin's definition of decentralization. The statement "the system being able to run in a scenario where each participant only has access to $O(c)$ resources" can be interpreted as a binary expression of whether the system can operate or not. However, if we consider the size of the "limited computational resources $O(c)$" as a variable, the ease of participation as a minor changes with the size of $O(c)$. This can be interpreted as the ease of each miner's entry into the system, which can be seen

as representing the degree of decentralization. Considering the relationship between decentralization as defined in Buterin's article on the trilemma and our conditions of decentralization, when it is easy to join the system (high decentralization as defined by Buterin's trilemma article), the number of nodes participating in the blockchain increases. Thus, the definitions of decentralization by Buterin and us are related.

In his blog post titled "The Meaning of Decentralization" [23], Buterin posits that decentralization can be divided along three axes, defining them as follows:

Architectural (de)centralization
: How many physical computers is a system made up of? How many of those computers can it tolerate breaking down at any single time?

Political (de)centralization
: How many individuals or organizations ultimately control the computers that the system is made up of?

Logical (de)centralization
: Does the interface and data structures that the system presents and maintains look more like a single monolithic object, or an amorphous swarm? One simple heuristic is: if you cut the system in half, including both providers and users, will both halves continue to fully operate as independent units?

However, these do not directly represent the decentralization discussed in Buterin's trilemma article. Rather than Buterin's definition of decentralization in the trilemma article, as stated in Section IV-A, our conditions for the decentralization index align with Buterin's "Architectural (de)centralization" and "Political (de)centralization".

3) SECURITY

In terms of security, Buterin's definition in the article on the trilemma [8] indicates a binary value of "whether it is safe against an attacker with resources up to $O(n)$." In contrast, our mathematical representation denotes the inverse of the fork rate, making our definition more specific and quantitative. In the paper [22], the "ratio of the total number of blocks in the main branch to the total number of confirmed blocks" has already been used as a metric for security. This metric closely aligns with the meaning of the fork rate, making the use of the inverse of the fork rate as a measure of security both standard and reasonable.

In his blog post titled "The Meaning of Decentralization" [23], Buterin describes the benefits of decentralization as follows:

Fault tolerance
: Decentralized systems are less likely to fail accidentally because they rely on many separate components that are not likely.

Attack resistance
: Decentralized systems are more expensive to attack and destroy or manipulate because they lack sensitive central points that can be attacked at much lower cost than the economic size of the surrounding system.

Collusion Resistance
: It is much harder for participants in decentralized systems to collude to act in ways that benefit them at the expense of other participants, whereas the leaderships of corporations and governments collude in ways that benefit themselves but harm less well-coordinated citizens, customers, employees, and the general public all the time.

In Buterin's definition of security, as stated "safe against an attacker with resources up to $O(n)$", the aforementioned benefits of decentralization, namely fault tolerance, attack resistance, and collusion resistance, are combined with other security elements (for instance, a high fork rate indicating network instability or increased success rates of Selfish Mining or Double Spending Attacks). In our definition, the benefits of decentralization manifest in the metrics for decentralization, allowing our definitions of security and decentralization to more appropriately distinguish between the two concepts.

B. THE DISCUSSION OF THE PARAMETERS AND ASSUMPTIONS OF TRILEMMA FORMULA

Here, we discuss parameters and assumptions that fall outside the scope set for deriving the trilemma formula.

1) QUANTIFICATION OF DECENTRALIZATION IN THE REAL WORLD

There could be some challenges in directly relating our trilemma formula to real-world decentralization indices because of the below differences between our model setting and the real world.

In Section II-A, we assume that nodes do not collude to derive the trilemma formula. However, in a real world, some nodes could collude.

Moreover, in Section V, we explore the correlation between decentralization and established decentralization indices. However, in the real world, the hash rates of individual nodes are unknown, making it difficult to determine these values. Therefore, because the hash rate share of a node relative to the entire network and the proportion of blocks that node has produced in the main chain are almost equal, the proportion of blocks produced by each node in the main chain is used to calculate decentralization indices in studies using existing decentralization indices [9].

Additionally, since it is challenging to obtain information on each individual node, mining pools are considered as single nodes, and decentralization indices are calculated using the proportion of blocks produced by each mining pool in the main chain.

These differences between the real world and our simulation may influence the relationship between existing decentralization indices and the terms indicating decentralization in the trilemma formula.

2) FORK CHOICE RULE

In our paper, we analyze the longest chain rule, which is the most popular fork choice rule adopted by Bitcoin. We will discuss the case of different fork choice rules. Under the longest chain rule, forks can significantly impact security because if an attacker tries to overtake the chain produced by honest nodes, any forks in the chain being extended by the honest nodes reduce the speed of chain growth, which benefits the attacker. On the other hand, choosing a fork choice rule that does not adopt the longest chain rule and reduces the impact of forks on security can mitigate security issues. For example, there is the GHOST [47] fork choice rule, which, unlike the longest chain rule that selects the longest chain, selects the heaviest chain by considering blocks in forks. This prevents an attacker's chain from gaining an advantage even if forks occur in the chain extended by honest nodes. The trilemma associated with other fork choice rules remains an open problem for future research.

3) THE RELATIONSHIP WITH SHARDING

In our paper, we derive the trilemma formula under the setting of one shard. Here, we discuss the relationship of this formula with Sharding. Sharding is a mechanism that divides a single blockchain into multiple smaller blockchains called shard chains. Each shard chain processes different data, improving scalability (throughput). Shards can be thought of as subsets of data and transactions from the original blockchain.

Firstly, our trilemma formula holds within each individual shard chain. However, according to our conditions for decentralization indices, when Sharding is introduced, decentralization is perceived to decrease. This is because the nodes that originally constituted a single blockchain are divided among shard chains, reducing the number of nodes in each individual shard chain. In fact, nodes that had a large hash rate before Sharding in an original blockchain, gain more influence within their respective shard chain after being allocated to it. Moreover, when viewed from the perspective of the entire blockchain, the influence of that node over certain data, such as ease of censorship, has also increased.

However, Buteirn's definition of decentralization in the trilemma, which means that ''the system being able to run in a scenario where each participant only has access to $O(c)$ resources'', differs from our definition of decentralization, which indicates the ''degree of influence distribution across the whole''. Therefore, Sharding becomes a means to solve the trilemma according to Buteirn's definition.

4) THE RELATIONSHIP WITH OFF-CHAIN CHANNELS

In our paper, we derived the trilemma formula on-chain. Here, we discuss the relationship between off-chain channels and our formula.

Off-chain channels, such as Lightning Network [48], are a technology that performs transactions outside of the blockchain, and at an appropriate stage, aggregates the results and records them on the blockchain. They are invented for improving scalability.

Off-chain channels allow parties to perform transactions an arbitrary number of times, recording only the final results on-chain. Thus, they increase the number of transactions that can be executed without violating our trilemma formula (i.e., without increasing the data size transmitted for consensus on the blockchain). This means that they do not impact the security or decentralization as defined by us on-chain.

On the other hand, it is necessary to consider the decentralization on off-chain platforms. Since our scope only includes the quantification of on-chain decentralization, we cannot quantify off-chain decentralization. However, we guess that in processing transactions, there is a degree of influence exerted by the nodes that make up the payment channels on the off-chain platform. If there are few nodes off-chain, the influence of the each nodes over the entire off-chain network in a transaction process increases. This can be considered low decentralization on off-chain platforms. The decentralization of off-chain channels remains an open problem.

5) OTHER SCALABILITY AND SECURITY PARAMETERS

In our trilemma formula, we regard tps as a scalability parameter and the inverse of fork rate as a security parameter. Here, we discuss the relationship with our formula and other scalability and security parameters.

a: OTHER SCALABILITY PARAMETERS

We consider TPS as a measure of scalability for deriving the trilemma formula because a higher TPS allows more users to perform transactions and is currently the most common index for assessing scalability. Although other measures for evaluating scalability are rarely used, Sanka and Cheung [12] have identified the size of storage required for node setup and read throughput as scalability indices. They argue that smaller required storage improves scalability because large storage requirements make it difficult for IoT devices and users to participate by setting up nodes. Our formula shows a proportional relationship between TPS and the size of storage required for node setup, as processing more transactions necessitates storing more data. Consequently, when our scalability is high, the scalability regarding the necessary storage size proposed by Sanka et al. is low. However, from the user's usage perspective, storing all blockchain data is not necessary even if the blockchain's transaction throughput increases.

Sanka and Cheung [12] also suggest that high read throughput improves scalability because IoT devices and users, instead of running full nodes, can fetch data from full nodes as needed. Read throughput is influenced by the number of full nodes in the network. Our formula does not include an element representing the number of full nodes, so it does not relate to this index.

b: OTHER SECURITY PARAMETERS

Regarding security indices, the success rates of Selfish Mining and Double Spending Attacks are sometimes calculated.

We discuss the relationship between these rates and the security term, the inverse of fork rate in our trilemma formula. Double Spending Attacks and Selfish Mining involve an attacker secretly building and extending a private chain hidden from honest nodes. The attacker reveals this private chain and replaces the main chain when it becomes as long as or longer than the honest chain. Thus, a higher fork rate, which implies a slower growth rate of the honest chain, increases the success rate of these attacks. This means that a smaller value of our formula's security term, i.e., a higher fork rate, correlates with higher success rates for Double Spending Attacks and Selfish Mining.

Moreover, it is obvious that the higher the hash rate β of an attacker, the greater the success rate of attacks like Selfish Mining and Double Spending Attack. The attacker's hash rate β tends to be higher in scenarios with lower levels of decentralization. In less decentralized contexts, nodes with larger hash rates exist, which are more likely to successfully attack than nodes with smaller hash rates, and thus more likely to become attackers. This indicates that lower decentralization leads to lower security, suggesting there is no trade-off between security and decentralization. However, one of the primary reasons for pursuing decentralization is to reduce the influence of individual nodes over the entire network, thereby preventing attacks from specific nodes [23]—decentralization is, in essence, a measure of security. Therefore, the trade-off between security and decentralization in our formula can also be interpreted as a trade-off between blockchain consensus security (the inverse of fork rate) and the security concerning decentralization.

IX. CONCLUSION

We have formulated an equation where the product of three terms representing decentralization, scalability, and security remains constant, allowing us to capture these properties as continuous variables rather than binary states. Furthermore, we have validated the trilemma formula in a simulator. Especially, we showed that $\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}$ represents decentralization, through both theory and experiments. Consequently, the impact of fluctuations in the decentralization term within the trilemma formula becomes more pronounced with a narrower range of node numbers or a larger range of bias. Moreover, the HHI is the most suitable exisisting decentralization index that meets our two conditions for a decentralization index. Our findings indicate that the decentralization term in the trilemma formula mirrors the HHI's representation of decentralization. Finally, we demonstrate two distinct methodologies for enhancing blockchain performance while adhering to the constraints outlined in the trilemma formula.

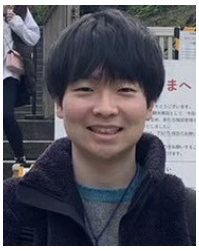
ACKNOWLEDGMENT

The authors would like to express their appreciation to Prof. Michinori Hatayama and Associate Professor Kohei Suenaga for their invaluable support and contributions to this research.

REFERENCES

[1] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Accessed: Jan. 2, 2024. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[2] M. Ur Rahman, F. Baiardi, and L. Ricci, "Blockchain smart contract for scalable data sharing in IoT: A case study of smart agriculture," in *Proc. IEEE Global Conf. Artif. Intell. Internet Things (GCAIoT)*, Dec. 2020, pp. 1–7.
[3] R. Nilaiswariya, J. Manikandan, and P. Hemalatha, "Improving scalability and security medical dataset using recurrent neural network and blockchain technology," in *Proc. Int. Conf. Syst., Comput., Autom. Netw. (ICSCAN)*, Jul. 2021, pp. 1–6.
[4] F. Tian, "A supply chain traceability system for food safety based on HACCP, blockchain & Internet of Things," in *Proc. Int. Conf. Service Syst. Service Manage.*, Jun. 2017, pp. 1–6.
[5] E. Androulaki, "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proc. 13th EuroSys Conf.*, New York, NY, USA, 2018, pp. 1–15.
[6] D. Schwartz, N. Youngs, and A. Britto, "The ripple protocol consensus algorithm," *Ripple Labs Inc. White Paper*, vol. 5, no. 8, p. 151, 2014.
[7] V. Buterin. (2015). *A Next Generation Smart Contract & Decentralized Application Platform*. Accessed: Jan. 3, 2024. [Online]. Available: https://api.semanticscholar.org/CorpusID:19568665
[8] V. Buterin. (2017). *Sharding FAQ, 2017*. Accessed: Dec. 2, 2024. [Online]. Available: https://vitalik.eth.limo/general/2017/12/31/sharding_faq.html
[9] Q. Lin, C. Li, X. Zhao, and X. Chen, "Measuring decentralization in Bitcoin and Ethereum using multiple metrics and granularities," in *Proc. IEEE 37th Int. Conf. Data Eng. Workshops (ICDEW)*, Apr. 2021, pp. 80–87.
[10] L. Zhang, X. Ma, and Y. Liu, "SoK: Blockchain decentralization," 2022, *arXiv:2205.04256*.
[11] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. Sirer, D. Song, and R. Wattenhofer, "On scaling decentralized blockchains," in *Financial Cryptography and Data Security*. Berlin, Germany: Springer, 1007, pp. 106–125.
[12] A. I. Sanka and R. C. C. Cheung, "A systematic review of blockchain scalability: Issues, solutions, analysis and future research," *J. Netw. Comput. Appl.*, vol. 195, Dec. 2021, Art. no. 103232.
[13] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2016, pp. 3–16.
[14] A. Fujihara, "Theoretical considerations on Bitcoin scalability problem and block size distribution," in *Proc. Blockchain Kaigi (BCK)*, 2022, Art. no. 011007.
[15] Y. Sompolinsky, Y. Lewenberg, and A. Zohar, "Spectre: A fast and scalable cryptocurrency protocol," *IACR Cryptol. ePrint Arch.*, vol. 2016, p. 1159, 2016. [Online]. Available: https://api.semanticscholar.org/CorpusID:20050445
[16] J. Wang and H. Wang, "Monoxide: Scale out blockchains with asynchronous consensus zones," in *Proc. 16th USENIX Symp. Networked Syst. Design Implement. (NSDI)*, 2019, pp. 95–112.
[17] A. Liu, Y. Liu, Q. Wu, B. Zhao, D. Li, Y. Lu, R. Lu, and W. Susilo, "CHERUBIM: A secure and highly parallel cross-shard consensus using quadruple pipelined two-phase commit for sharding blockchains," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 3178–3193, 2024.
[18] L. T. Thibault, T. Sarry, and A. S. Hafid, "Blockchain scaling using rollups: A comprehensive survey," *IEEE Access*, vol. 10, pp. 93039–93054, 2022.
[19] A. P. Ozisik, G. Andresen, B. N. Levine, D. Tapp, G. Bissias, and S. Katkuri, "Graphene: Efficient interactive set reconciliation applied to blockchain propagation," in *Proc. ACM Special Interest Group Data Commun.*, Aug. 2019, pp. 303–317.
[20] E. Georgiadis, "How many transactions per second can Bitcoin really handle ? Theoretically," *IACR Cryptol. ePrint Arch.*, vol. 2019, p. 416, 2019. [Online]. Available: https://api.semanticscholar.org/CorpusID:150371894
[21] J. Werth, M. Berenjestanaki, H. Barzegar, N. El Ioini, and C. Pahl, "A review of blockchain platforms based on the scalability, security and decentralization trilemma," in *Proc. 25th Int. Conf. Enterprise Inf. Syst.*, 2023, pp. 146–155.
[22] X. Zheng, Y. Zhu, and X. Si, "A survey on challenges and progresses in blockchain technologies: A performance and security perspective," *Appl. Sci.*, vol. 9, no. 22, p. 4731, Nov. 2019.
[23] V. Buterin. (2017). *The Meaning of Decentralization*. Accessed: Aug. 26, 2023. [Online]. Available: https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

[24] M. Zamani, M. Movahedi, and M. Raykova, "RapidChain: Scaling blockchain via full sharding," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2018, pp. 931–948.
[25] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, "Algorand: Scaling Byzantine agreements for cryptocurrencies," in *Proc. 26th Symp. Operating Syst. Princ.*, Oct. 2017, pp. 51–68.
[26] M. Conti, A. Gangwal, and M. Todero, "Blockchain trilemma solver algorand has dilemma over undecidable messages," in *Proc. 14th Int. Conf. Availability, Rel. Secur.*, Aug. 2019, pp. 1–8.
[27] Trifecta Blockchain Team. (2021). *Trifecta: The Blockchain Trilemma Solved*. Accessed: Feb. 25, 2024. [Online]. Available: https://api.semanticscholar.org/CorpusID:231844745
[28] V. Bagaria, S. Kannan, D. Tse, G. Fanti, and P. Viswanath, "Prism: Deconstructing the blockchain to approach physical limits," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, New York, NY, USA, Nov. 2019, pp. 585–602.
[29] H. Wang, H. Li, A. Smahi, M. Xiao, and S.-Y. R. Li, "GBT-CHAIN: A system framework for solving the general trilemma in permissioned blockchains," *Distrib. Ledger Technol.*, early access, Aug. 2023. [Online]. Available: https://dl.acm.org/doi/10.1145/3615871
[30] S. Chu and S. Wang, "The curses of blockchain decentralization," 2018, *arXiv:1810.02937*.
[31] J. Albrecht, S. Andreina, F. Armknecht, G. Karame, G. Marson, and J. Willingmann, "Larger-scale Nakamoto-style blockchains don't necessarily offer better security," 2024, *arXiv:2404.09895*. [Online]. Available: https://arxiv.org/abs/2404.09895
[32] T. Nakai, A. Sakurai, S. Hironaka, and K. Shudo, "The blockchain trilemma described by a formula," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Dec. 2023, pp. 41–46.
[33] A. Sakurai and K. Shudo, "Impact of the hash rate on the theoretical fork rate of blockchain," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2023, pp. 1–4.
[34] Y. Aoki, K. Otsuki, T. Kaneko, R. Banno, and K. Shudo, "SimBlock: A blockchain network simulator," in *Proc. IEEE INFOCOM Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Apr. 2019, pp. 325–329.
[35] R. Nagayama, R. Banno, and K. Shudo, "Identifying impacts of protocol and Internet development on the Bitcoin network," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jul. 2020, pp. 1–6.
[36] *Bitnodes*. Accessed: Aug. 3, 2024. [Online]. Available: https://bitnodes.io/
[37] *Wondernetwork*. Accessed: Aug. 3, 2024. [Online]. Available: https://wondernetwork.com/
[38] *Testmy.net*. Accessed: Mar. 8, 2024. [Online]. Available: https://testmy.net/
[39] S. Delgado-Segura, S. Bakshi, C. Pérez-Solà, J. Litton, A. Pachulski, A. Miller, and B. Bhattacharjee, "TxProbe: Discovering Bitcoin's network topology using orphan transactions," in *Proc. FC*, 2019, pp. 550–566.
[40] C. Gini, "Concentration and dependency ratios," *Rivista di Politica Economica*, vol. 87, pp. 769–789, Jan. 1909.
[41] B. S. Srinivasan and L. Lee. (2017). *Quantifying Decentralization, 2017*. Accessed: Aug. 30, 2023. [Online]. Available: https://news.earn.com/quantifying-decentalization-e39db233c28e
[42] (2023). *Bitcoin Visuals*. Accessed: Jul. 12, 2023. [Online]. Available: https://bitcoinvisuals.com/chain-tx-size
[43] M. Corallo. (2016). *Compact Block Relay*. Accessed: Aug. 25, 2023. [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0152.mediawiki
[44] T. Hasegawa, A. Sakurai, and K. Shudo, "Quick notification of block generation using Bloom filter in a blockchain," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jul. 2023, pp. 457–463.
[45] R. Pass and E. Shi, "FruitChains: A fair blockchain," in *Proc. ACM Symp. Princ. Distrib. Comput.*, Jul. 2017, pp. 315–324.
[46] Y. Aoki and K. Shudo, "Proximity neighbor selection in blockchain networks," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Jul. 2019, pp. 52–58.
[47] Y. Sompolinsky and A. Zohar, "Secure high-rate transaction processing in Bitcoin," in *Proc. 19th Int. Conf. Financial Cryptogr. Data Secur.*, 2015, pp. 507–527.
[48] J. Poon and T. Dryja, "The Bitcoin lightning network: Scalable off-chain instant payments," White Paper, 2016. [Online]. Available: https://static1.squarespace.com/static/6148a75532281820459770d1/t/61af971f7ee2b432f1733aee/1638897446181/lightning-network-paper.pdf



TAISHI NAKAI received the B.E. degree in engineering and the M.E. degree in informatics from Kyoto University, Japan, in 2022 and 2024, respectively, where he is currently pursuing the Ph.D. degree. His research interest includes distributed ledger technologies.

AKIRA SAKURAI received the B.S. and M.S. degrees in science from Tokyo Institute of Technology, in 2022 and 2024, respectively. He is currently pursuing the Ph.D. degree with Kyoto University. His research interest includes distributed systems, especially cryptocurrency.

SHIORI HIRONAKA received the B.E., M.E., and Ph.D. degrees in engineering from Toyohashi University of Technology, Japan, in 2016, 2018, and 2021, respectively. She is currently an Assistant Professor with the Academic Center for Computing and Media Studies, Kyoto University. Her research interests include social media mining, graph analysis, and computational social science.

KAZUYUKI SHUDO (Senior Member, IEEE) received the B.E., M.E., and Ph.D. degrees in computer science from Waseda University, in 1996, 1998, and 2001, respectively. He was a Research Associate with Waseda University, from 1998 to 2001. He was a Research Scientist with the National Institute of Advanced Industrial Science and Technology. In 2006, he joined as the Director and the Chief Technology Officer with Utagoe Inc. Since December 2008, he has been an Associate Professor with Tokyo Institute of Technology. Since April 2022, he has been a Professor with Kyoto University. His research interests include distributed computing, programming language systems, and information security. He is a member of the IEEE Communications Society, the IEEE Computer Society, and ACM.