The Blockchain Trilemma Described by a Formula

Taishi Nakai
Kyoto University
Kyoto, Japan

Akira Sakurai
Tokyo Institute of Technology
Tokyo, Japan

Shiori Hironaka
Kyoto University
Kyoto, Japan

Kazuyuki Shudo
Kyoto University
Kyoto, Japan

***Abstract*—The blockchain trilemma was first introduced in a 2017 blog post written by Vitalik Buterin, one of the co-founders of Ethereum. This trilemma claims that it is impossible to simultaneously achieve the three properties of decentralization, scalability, and security in a blockchain. While extensive analysis of blockchain performance has been conducted, the claim has been empirically accepted as true. However, no one has formulated this trilemma mathematically. In this paper, we present a formula that explicitly expresses the trilemma for Proof of Work blockchains. Furthermore, based on our mathematical representation of the trilemma, we illustrate the two categories of approaches for improving blockchain performance under the constraints of the trilemma.**

***Index Terms*—blockchain, trilemma, decentralization, scalability, security**

I. Introduction

Blockchain is a distributed ledger that became widely known when Satoshi Nakamoto published a paper on Bitcoin in 2008 [1]. Blockchain is characterized by its decentralization and high security. However, compared with traditional databases, blockchains have lower processing performance, scalability. There have been many studies to improve its scalability. For instance, Fast Coin [2] improves scalability by reducing the block propagation time and SPECTRE [3] by using a Directed Acyclic Graph for its consensus algorithm. In addition, sharding, as seen in RapidChain [4], distributes transactions across multiple groups of nodes, and Rollup [5] processes transactions off-chain to improve scalability. There are also studies, such as Compact Block Relay [6], that aim to increase scalability by reducing the size of propagated blocks.

In 2017, Vitalik Buterin, one of the co-founders of Ethereum [7], wrote in a blog post [8] that a blockchain can achieve at most two out of the following three properties: decentralization, scalability, and security. This concept is known as the blockchain trilemma, which is shown in Figure 1. Buterin defined the three properties as follows:

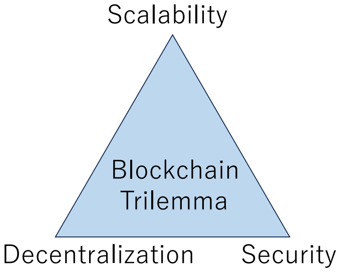

Fig. 1. Blockchain Trilemma.

Decentralization
: 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
: defined as being able to process $O(n) > O(c)$ transactions.

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

where c denotes the size of computational resources (including computation, bandwidth, and storage) available to each node, and n denotes 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.

Under Buterin's definition of trilemma, while Bitcoin achieves decentralization and security, it does not meet the criteria for scalability. According to a paper that calculated the maximum transaction throughput for Bitcoin [9], Bitcoin can only process a maximum of 27 transactions per second. This is clearly below the number of transactions that a normal computer can process.

This trilemma has been empirically recognized as accurate with the increasing analysis of blockchain. However, the trilemma and its three properties are not well defined, such as by mathematical formulas, and the current situation is that different definitions are adopted depending on the individual. As a result, it is unclear whether research on scalability improvements can improve scalability without negatively impacting decentralization or security. There have been instances where it has been touted that the constraints of the trilemma have been resolved, leading to an improvement in the processing performance of the blockchain. Moreover, while Buterin's definition of the three properties of the trilemma is binary, more precisely, the three properties have a inverse relationship. For instance, according to Buterin's definition, Bitcoin has not achieved scalability. In reality, if you compromise on security or decentralization to a certain extent, scalability increases proportionally to the level of compromise. Therefore, Buterin's definition does not strictly represent the trilemma.

[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.

Proc. 6th IEEE Int'l Conf. on Blockchain
(IEEE Blockchain 2023), pp.41-46, December 2023

In this paper, we demonstrate mathematically a trilemma for blockchains employing Proof of Work by deriving a formula where the product of three continuous non-binary quantities, decentralization, scalability, and security, remains constant. We also compare the properties of Buterin's trilemma with the properties presented in our formula. Furthermore, from our trilemma formula, we demonstrate that there are two distinct approaches to improve the performance of the blockchain while satisfying the constraints of the trilemma. continuous non-binary quantities,

II. Mathematical Description of the Trilemma

We derive a formula that expresses the trilemma, scalability × security × decentralization = constant, by transforming the equations that express the fork rate and the average block propagation time weighted by the hash rate, as defined in Sakurai et al.'s study [10].

First, we explain the definition of the average block propagation time weighted by the hash rate, T_w. Second, we represent T_w, which was conveniently expressed as continuous form in Sakurai et al.'s paper [10], more accurately as the sum of discrete values. Finally, we derive the formula representing the trilemma from T_w and other equations.

A. Explanation of the Average Block Propagation Time Weighted by the Hash Rate

We explain the average block propagation time weighted by the hash rate, T_w, as defined by Sakurai et al. [10]. We first describe the average block propagation time weighted by the hash rate for node i, $T_{w,i}$.

$T_{w,i}$ is the sum of the time it took for a block generated by node i to reach a certain node, multiplied by that node's hash rate proportion, summed across all nodes. Figure 2 provides an example of a graph where the horizontal axis represents the elapsed time since the block is generated, and the vertical axis represents the total hash rate of miners that have received the block up to that time. The average block propagation time weighted by the hash rate for node i, $T_{w,i}$, is represented by the area of the red shaded region in the graph. $T_{w,i}$ is expressed by the following equation:

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

where $u_i(t)$ denotes the total proportion of the hash rate of nodes that have not received the block t units of time after node i successfully generated the block. In addition, $u_i'(t)$ represents the derivative of $u_i(t)$. In reality, $u_i(t)$ might not be differentiable, but for simplicity, $u_i(t)$ is treated as differentiable in this context.

Considering the moment each node generates a block, 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 expressed by the following equation:

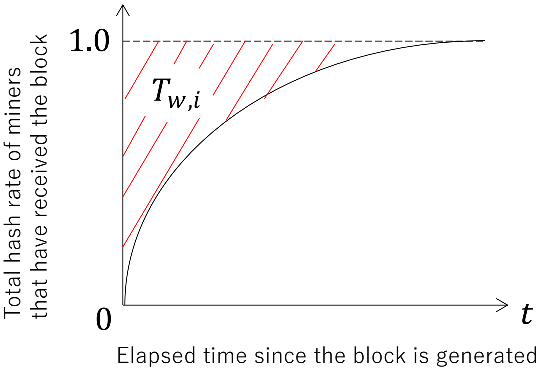

Fig. 2. Visualization of $T_{w,i}$. Total hash rate of miners that have received the block before time t versus the elapsed time since the block is generated by node i. The area of the red shaded region is $T_{w,i}$.

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

where n denotes the number of nodes participating in the network, and H_i is the proportion of the hash rate that node i possesses relative to the entire network's hash rate.

Furthermore, based on the definition of H_i, the following equation holds.

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

B. Representation of the Average Block Propagation Time Weighted by the Hash Rate, T_w, as a Sum of Discrete Values

We express the average block propagation time weighted by the hash rate T_w as a sum of discrete values. In the paper of Sakurai et al. [10], T_w was calculated using integration, assuming the propagation time for each node as a continuous function. However, in reality, the propagation time for each node is not a continuous function. Therefore, we represent T_w using discrete values.

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, is defined as the average block propagation time weighted by the hash rate for node i, $T_{w,i}$. If T_{ij} is the time taken for the block generated by node i to propagate to node j, then $T_{w,i}$ can be expressed by the following equation. In this context, it is assumed that there is no block propagation from node i to itself.

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

We derive T_w from $T_{w,i}$. 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 equation (4), the average block propagation time weighted by the hash rate T_w can be expressed by the following equation.

$$\begin{aligned} T_w &= \sum_{i=1}^{n} H_i T_{w,i} \\ &= \sum_{i=1}^{n} H_i \sum_{j=1, j\neq i}^{n} H_j T_{ij} \end{aligned} \tag{5}$$

C. Derivation of the Trilemma

When the block size is B and the time taken for a block generated by node i to propagate to node j per byte is t_{ij}, Equation (5) can be represented by the following expression.

$$\begin{aligned} T_w &= \sum_{i=1}^{n} H_i \sum_{j=1, j\neq i}^{n} H_j \cdot B \cdot t_{ij} \\ &= B \sum_{i=1}^{n} H_i \sum_{j=1, j\neq i}^{n} H_j t_{ij} \end{aligned} \tag{6}$$

Since equation (6) is a quadratic form (a polynomial consisting only of quadratic terms), it can be represented using a vector $\boldsymbol{H}$ that describes the distribution of hash rates and a matrix $\boldsymbol{P}$ whose elements represent the block propagation times between each pair of nodes.

$$T_w = B\boldsymbol{H}^\top \boldsymbol{P} \boldsymbol{H} \tag{7}$$

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

$$\boldsymbol{H} = \begin{pmatrix} H_1 \\ H_2 \\ \vdots \\ H_n \end{pmatrix} \tag{8}$$

$$\boldsymbol{P} = \begin{pmatrix} 0 & t_{12} & \dots & t_{1n} \\ t_{21} & 0 & \dots & t_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ t_{n1} & t_{n2} & \dots & 0 \end{pmatrix} \tag{9}$$

$\boldsymbol{H}^\top$ denotes the transposed vector of $\boldsymbol{H}$. In the matrix $\boldsymbol{P}$, the diagonal elements indicate the time taken for the block propagation to itself. Since a block does not propagate between identical nodes, these diagonal elements are set to 0.

Calculated by Sakurai et al [10], the theoretical fork rate F can be represented using the block generation interval T and the average block propagation time weighted by the hash rate T_w as follows.

$$F = \frac{T_w}{T} \tag{10}$$

Substitute Equation (7) into Equation (10).

$$F = \frac{B\boldsymbol{H}^\top \boldsymbol{P} \boldsymbol{H}}{T} \tag{11}$$

Furthermore, the block size B can be represented using the block header size B_h, the size of one transaction B_{tx}, and the number of transactions contained in one block n_{tx} as follows.

$$B = B_h + B_{tx} \cdot n_{tx} \tag{12}$$

By substituting equation (12) into equation (11) and transforming the equation under the condition $F \neq 0$, the following equation can be derived.

$$\frac{B_h + B_{tx} \cdot n_{tx}}{T} \cdot \frac{1}{F} \cdot \boldsymbol{H}^\top \boldsymbol{P} \boldsymbol{H} = 1 \tag{13}$$

In equation (13), $\frac{n_{tx}}{T}$ denotes the number of transactions that can be processed per unit of time, commonly referred to as Transactions Per Second (TPS). The TPS is often used as a measure of scalability [11]. Thus, the first fraction includes a representation of scalability when assuming B_h and B_{tx} are constants and TPS is a metric for scalability. Additionally, a high fork rate complicates the decision for miners on which branch to adopt. This fragmentation of the hash rate can lead to increased security risks, such as Double Spending Attack and Selfish Mining [12]. Therefore, the inverse of the fork rate ($\frac{1}{F}$) can be interpreted as a representation and metric of security. If B_h and B_{tx} are constants, and if we consider $\boldsymbol{H}^\top \boldsymbol{P} \boldsymbol{H}$ as a property for decentralization, equation (13) expresses that the product of the three metrics representing scalability, security, and decentralization is equal to 1. This implies that it is difficult to improve all three elements simultaneously, which is precisely the essence of the trilemma. The decentralization exhibited by $\boldsymbol{H}^\top \boldsymbol{P} \boldsymbol{H}$ is discussed in Section III. B_h and B_{tx}, which are constants here, are also examined in Section V-A.

III. Examination of Indicators Representing Decentralization

We explore the possibility that $\boldsymbol{H}^\top \boldsymbol{P} \boldsymbol{H}$ indicates decentralization. First, we show that $\boldsymbol{H}$ represents a property of decentralization, and this decentralization can be evaluated by the variance of the elements of $\boldsymbol{H}$, $\mathrm{Var}[\boldsymbol{H}]$. Second, we demonstrate that the decentralization of $\boldsymbol{H}$ indicates through $\boldsymbol{H}^\top \boldsymbol{P} \boldsymbol{H}$.

A. Decentralization Indicated by $\boldsymbol{H}$ and the metric $\mathrm{Var}[\boldsymbol{H}]$

The higher the decentralization, the more evenly distributed the hash rate is across each node and the greater the number of nodes constituting the blockchain network as illustrated in Figure 3. If there is a bias in the hash rates or if the number of nodes is limited, the benefits of decentralization such as fault tolerance, attack resistance, and collusion resistance diminish, as discussed in [13]. The vector $\boldsymbol{H}$ represents the distribution of the hash rate of nodes, and its dimension inherently indicates the number of nodes n, making it a direct representation of decentralization.

Proc. 6th IEEE Int'l Conf. on Blockchain
(IEEE Blockchain 2023), pp.41-46, December 2023

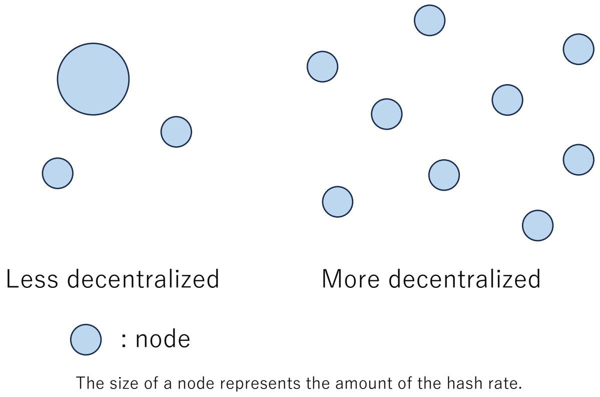

Fig. 3. Decentralization illustrated.

To evaluate the decentralization represented by vector $\boldsymbol{H}$, we compute the variance of its elements. The average of the elements of $\boldsymbol{H}$, denoted as $\mathrm{Avg}[\boldsymbol{H}]$, is given by:

$$\begin{aligned}\mathrm{Avg}[\boldsymbol{H}] &= \frac{\sum_{i=1}^{n} H_i}{n} \\ &= \frac{1}{n}.\end{aligned} \tag{14}$$

Consequently, the variance of the elements of $\boldsymbol{H}$, denoted as $\mathrm{Var}[\boldsymbol{H}]$, can be expressed as:

$$\begin{aligned}\mathrm{Var}[\boldsymbol{H}] &= \frac{\sum_{i=1}^{n} {H_i}^2}{n} - (\mathrm{Avg}[\boldsymbol{H}])^2 \\ &= \frac{1}{n}\sum_{i=1}^{n} {H_i}^2 - \frac{1}{n^2}.\end{aligned} \tag{15}$$

The maximum and minimum values of $\mathrm{Var}[\boldsymbol{H}]$ are:

$$0 \leq \mathrm{Var}[\boldsymbol{H}] \leq \frac{1}{n} - \frac{1}{n^2}. \tag{16}$$

When all n nodes possess an equal hash rate, implying the highest decentralization from the perspective of hash rate distribution, with $H_i = \frac{1}{n}(i = 1, \ldots, n)$, $\mathrm{Var}[\boldsymbol{H}]$ takes its minimum value of 0. Conversely, considering the scenario with the lowest decentralization from the perspective of hash rate distribution, where only one node in n nodes holds the entire hash rate of 1 and all other nodes have a hash rate of 0, $\mathrm{Var}[\boldsymbol{H}]$ takes its maximum value of $\frac{1}{n} - \frac{1}{n^2}$.

Furthermore, under the condition of equation (3), in situations where the number of nodes n is large, implying higher decentralization, $\mathrm{Var}[\boldsymbol{H}]$ becomes smaller. Conversely, when n is small, indicating lower decentralization, $\mathrm{Var}[\boldsymbol{H}]$ becomes larger.

Thus, the smaller the statistical variance $\mathrm{Var}[\boldsymbol{H}]$, the greater the decentralization of the blockchain. This confirms that the vector $\boldsymbol{H}$ represents an element of decentralization, and $\mathrm{Var}[\boldsymbol{H}]$ serves as a metric indicating decentralization.

B. Decentralization Indicated by $\boldsymbol{H}$ through $\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}$

We aim to demonstrate how the decentralization represented by $\boldsymbol{H}$ is indicated through $\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}$.

$\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}$ is a quadratic form and can be expressed without vectors and matrices as:

$$\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H} = \sum_{i=1}^{n} \sum_{j=1, j\neq i}^{n} t_{ij} H_i H_j. \tag{17}$$

We consider the case where the block propagation time t_{ij} is the same for all nodes. That is, each element of matrix $\boldsymbol{P}$ is constant at t_c. Then, we aim to determine the maximum and minimum values of $\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}$, as well as the vector $\boldsymbol{H}$ that represents the distribution of hash rates when these maximum and minimum values are achieved. In this process, we utilize equation (3) for algebraic manipulations.

$$\begin{aligned}\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H} &= \sum_{i=1}^{n} \sum_{j=1, j\neq i}^{n} t_c H_i H_j \\ &= t_c \sum_{i=1}^{n} \sum_{j=1, j\neq i}^{n} H_i H_j \\ &= t_c \sum_{i=1}^{n} H_i \left(\sum_{j=1}^{n} H_j - H_i \right) \\ &= t_c \sum_{i=1}^{n} H_i \left(1 - H_i\right) \\ &= t_c \left(1 - \sum_{i=1}^{n} {H_i}^2 \right)\end{aligned} \tag{18}$$

From the above equation, the maximum and minimum values of $\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}$ can be expressed as:

$$0 \leq \boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H} \leq t_c \left(1 - \frac{1}{n}\right). \tag{19}$$

When all n nodes have the same hash rate, implying maximum decentralization, $H_i = \frac{1}{n}(i = 1, \ldots, n)$, $\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}$ reaches its maximum value of $t_c \left(1 - \frac{1}{n}\right)$. If one of the n nodes possesses all the hash rate 1, and all other nodes have a hash rate of 0, implying minimum decentralization, $\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}$ takes its minimum value of 0.

Furthermore, under the conditions of equation (3), when the number of nodes n is large, indicating high decentralization, $\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}$ becomes larger. Conversely, when n is small, indicating low decentralization, $\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}$ becomes smaller.

Thus, in situations where there is no bias in propagation speed between nodes, when the blockchain's decentralization is high, $\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}$ becomes larger, and when the decentralization is low, $\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}$ becomes smaller.

In equation (15), $\mathrm{Var}[\boldsymbol{H}]$ becomes smaller in highly decentralized situations and larger in less decentralized situations. On the other hand, $\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}$ becomes larger in highly decentralized situations and smaller in less decentralized ones. This is due to the $\sum_{i=1}^{n} {H_i}^2$ part appearing in both equations (15) and (18), and in equation (18), it has a negative sign. Therefore, the property of $\boldsymbol{H}$ indicating decentralization is reflected in $\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}$ in the same way as $\mathrm{Var}[\boldsymbol{H}]$.

In summary, it can be seen that if the block propagation time t_{ij} is the same for all nodes, then $\boldsymbol{H}$ indirectly indicates decentralization through $\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}$.

For interpretations regarding the situation where the block propagation time t_{ij} is not equal between each node, see Section V-B.

IV. Comparison with the Three Properties of Buterin's Trilemma

We compare the properties of the trilemma defined in formula (13) with the properties of Buterin's trilemma. Table I organizes the three properties of Buterin and those defined in our mathematical formulation.

A. Scalability Comparison

Unlike the existing definition by Buterin, we have adopted TPS (Transactions Per Second) as the definition of scalability. This definition provides specific and quantitative information, and is commonly used to measure the scalability of a chain [11].

B. Decentralization Comparison

According to Buterin's definition, if one node controls the hash rate of the entire system, and if each miner can only access resources of $O(c)$, or if the system is easy to join, then this scenario must be rated as highly decentralized. However, this is clearly a centralized state. On the other hand, even in this scenario, our metric $\mathrm{Var}[\boldsymbol{H}]$ increases (indicating our lower decentralization), making it more appropriate to depict decentralization.

C. Security Comparison

In Buterin's article on the trilemma [8], the definition indicates whether a system is safe against an attacker with resources up to $O(n)$. Our metric, on the other hand, indicates the "inverse of the fork rate", making our definition more specific and quantitative. In the paper [14], 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 is close in meaning to the fork rate, making it common and reasonable to use the inverse of the fork rate as a security indicator.

In conclusion, for the three elements of scalability, decentralization, and security, Vitalik's definitions are binary and vague. In contrast, our definitions excel in being more specific and quantitative.

V. Two approaches to improve blockchain performance under the constraints of the trilemma

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

A. Approaches to Reduce B_h and B_{tx}

In Section II-C, we identified the trilemma within equation (13) by assuming B_h and B_{tx} to be constant. Here, we abandon the assumption of constancy for B_h and B_{tx} in equation (13) and aim to reduce them.

In equation (13), when we reduce B_h and B_{tx}, it does not adversely affect $\frac{n_{tx}}{T}$, $\frac{1}{F}$, and the distribution of $\boldsymbol{H}$. As a result, 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 performance within the constraints of the trilemma. For instance, Bitcoin's Compact Block Relay [6] and the optimization of block generation notifications in the blockchain using bloom filters [15] improve blockchain performance by reducing B_h and B_{tx}.

B. Optimization of Elements within $\boldsymbol{P}$

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

Focusing on Equation (17), 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 blockchain performance within the constraints of the trilemma. For instance, in the selection of neighboring nodes [16], the performance 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 blockchain's performance, even within the constraints of the trilemma. Moreover, in Bitcoin's Compact Block Relay [6], the performance of the blockchain is improved by sending sketches to related nodes before block verification is complete.

Looking again at equation (17), especially between nodes where the product of two hash rates is large, improving 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 III-B, we assume that the block propagation time between each node is equal. If the block propagation time varies between nodes, as demonstrated in this subsection, $\boldsymbol{H}^\top \boldsymbol{P}\boldsymbol{H}$, which indirectly indicates the decentralization of H, increase or decrease depending on the block propagation time between each node.

VI. Conclusion

We represented the trilemma of the blockchain mathematically by deriving a formula where the product of the three

TABLE I
COMPARISON OF TRILEMMA'S THREE PROPERTIES BETWEEN BUTERIN AND OUR MATHEMATICAL FORMULATION.

Property	Buterin's Definition	Our metrics
Scalability	Defined as being able to process $O(n)$[a]$> O(c)$[b]transactions.	Number of transactions that can be processed per unit time(TPS).
Decentralization	Defined as the system being able to run in a scenario where each participant only has access to $O(c)$ resources, i.e. a regular laptop or small Virtual Private Server.	The abundance of nodes and the lack of bias in the distribution of the hash rate (Variance of hash rate, $\mathrm{Var}[\boldsymbol{H}]$).
Security	Defined as being secure against attackers with up to $O(n)$ resources.	Difficulty in causing forks (inverse of fork rate F).

[a] n denotes 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.

[b] c denotes the size of computational resources (including computation, bandwidth, and storage) available to each node.

continuous quantities: scalability, security, and decentralization, remains constant. Unlike Buterin's binary definition, this formula illustrates the inverse relationship among the three continuous variables, offering a more precise representation of the trilemma. We demonstrated that $\boldsymbol{H}$ represents an property of decentralization, and this decentralization can be evaluated using the metric $\mathrm{Var}[\boldsymbol{H}]$. Furthermore, we showed that the decentralization of $\boldsymbol{H}$ is expressed through $\boldsymbol{H}^{\top}\boldsymbol{P}\boldsymbol{H}$ in the same manner as $\mathrm{Var}[\boldsymbol{H}]$. We compared the three properties of the trilemma as defined by Buterin with those in our mathematical formula. Additionally, from our formula, we have shown that there are two categories of approach to enhance the performance of the blockchain while adhering to the constraints of the trilemma.

In Section V, "Two Approaches to improve blockchain performance under the constraints of the trilemma", and specifically in Section V-B, "Optimization of Elements within $\boldsymbol{P}$", we mentioned that by improving communication performance, particularly between nodes with a high product of hash rates, the performance of the blockchain can be effectively enhanced under the constraints of the trilemma. However, by reducing the block propagation time between specific pairs of nodes compared to others, these nodes might gain an advantage in mining. We will further examine the possibility that this approach might adversely affect the blockchain in future research.

While our study focused on blockchains adopting Proof of Work, we also plan to mathematically represent the trilemma for blockchains that adopt Proof of Stake.

ACKNOWLEDGMENT

This work was supported by JSPS KAKENHI Grant Number JP21H04872.

REFERENCES

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[2] Yonatan Sompolinsky and Aviv Zohar. Secure high-rate transaction processing in bitcoin. In Rainer Böhme and Tatsuaki Okamoto, editors, *Financial Cryptography and Data Security*, pages 507–527, Berlin, Heidelberg, 2015. Springer Berlin Heidelberg.

[3] Yonatan Sompolinsky, Yoad Lewenberg, and Aviv Zohar. Spectre: A fast and scalable cryptocurrency protocol. Cryptology ePrint Archive, Paper 2016/1159, 2016. https://eprint.iacr.org/2016/1159.

[4] Mahnush Movahedi Mahdi Zamani and Mariana Raykova. Rapidchain: Scaling blockchain via full sharding. In *Proceedings of the 2018 ACM SIGSAC conference on computer and communications security*, pages 931–948, 2018.

[5] Tom Sarry Louis Tremblay Thibault and Abdelhakim Senhaji Hafid. Blockchain scaling using rollups: A comprehensive survey. *IEEE Access*, 10:93039–93054, 2022.

[6] Matt Corallo. Compact block relay, 2016. https://github.com/bitcoin/bips/blob/master/bip-0152.mediawiki, (Accessed on 08/25/2023).

[7] Vitalik Buterin et al. A next-generation smart contract and decentralized application platform. *white paper*, 3(37):2–1, 2014.

[8] Vitalik Buterin. Sharding FAQ, 2017. https://vitalik.ca/general/2017/12/31/sharding_faq.html, (Accessed on 08/17/2023).

[9] Evangelos Georgiadis. How many transactions per second can bitcoin really handle ? theoretically. Cryptology ePrint Archive, Paper 2019/416, 2019. https://eprint.iacr.org/2019/416.

[10] Akira Sakurai and Kazuyuki Shudo. Impact of the hash rate on the theoretical fork rate of blockchain. In *IEEE ICCE 2023*, pages 1–4. IEEE, 2023.

[11] Abdurrashid Ibrahim Sanka and Ray C.C. Cheung. A systematic review of blockchain scalability: Issues, solutions, analysis and future research. *Journal of Network and Computer Applications*, 195:103232, 2021.

[12] Arthur Gervais, Ghassan O. Karame, Karl Wüst, Vasileios Glykantzis, Hubert Ritzdorf, and Srdjan Capkun. On the security and performance of proof of work blockchains. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, pages 3–16, 2016.

[13] Vitalik Buterin. The meaning of decentralization, 2017. https://medium.com/@VitalikButerin//the-meaning-of-decentralization-a0c92b76a274, (Accessed on 08/26/2023).

[14] Xiaoying Zheng, Yongxin Zhu, and Xueming Si. A survey on challenges and progresses in blockchain technologies: A performance and security perspective. *Applied Sciences*, 9(22):4731, 2019.

[15] Tsuyoshi Hasegawa, Akira Sakurai, and Kazuyuki Shudo. Quick notification of block generation using bloom filter in a blockchain. In *2023 IEEE Symposium on Computers and Communications (ISCC)*, pages 457–463, 2023.

[16] Yusuke Aoki and Kazuyuki Shudo. Proximity neighbor selection in blockchain networks. In *2019 IEEE International Conference on Blockchain (Blockchain)*, pages 52–58, 2019.

Proc. 6th IEEE Int'l Conf. on Blockchain
(IEEE Blockchain 2023), pp.41-46, December 2023