The Rich Get Richer in Bitcoin Mining Induced by Blockchain Forks

Akira Sakurai
Kyoto University
Kyoto, Japan

Kazuyuki Shudo
Kyoto University
Kyoto, Japan

***Abstract*—Bitcoin is a representative decentralized currency system. For the security of Bitcoin, fairness in the distribution of mining rewards plays a crucial role in preventing the concentration of computational power in a few miners. Here, fairness refers to the distribution of block rewards in proportion to contributed computational resources. If miners with greater computational resources receive disproportionately higher rewards—i.e., if the "Rich Get Richer" (TRGR) phenomenon holds in Bitcoin—it indicates a threat to the system's decentralization. This study analyzes TRGR in Bitcoin by focusing on unintentional blockchain forks, an inherent phenomenon in Bitcoin. Previous research has failed to provide generalizable insights due to the low precision of their analytical methods. In contrast, we avoid this problem by adopting a method whose analytical precision has been empirically validated. The primary contribution of this work is a theoretical analysis that clearly demonstrates TRGR in Bitcoin under the assumption of fixed block propagation delays between different miners. More specifically, we show that the mining profit rate depends linearly on the proportion of hashrate. Furthermore, we examine the robustness of this result from multiple perspectives in scenarios where block propagation delays between different miners are not necessarily fixed.**

***Index Terms*—Bitcoin, Blockchain Forks, Mining Fairness, The Rich Get Richer (TRGR)**

I. Intruduction

Bitcoin [1] is a peer-to-peer currency system that enables transactions without relying on a trusted third party. In the Bitcoin protocol, nodes that process transactions are referred to as miners. Anyone can become a miner, and miners are incentivized to follow the protocol, thereby eliminating the need for users to trust any centralized authority when processing transactions.

From a security perspective, it is essential that computational resources (i.e., hashrate) are not concentrated in Bitcoin. Concretely, the protocol assumes that the majority of computational resources are held by honest miners in order for transactions to be securely processed. For example, if a particular miner gains control of more than 51% of the network's total hashrate, they could arbitrarily alter transaction histories [2] [3] [4]. Even when this threshold is not surpassed, attacks such as selfish mining [5] become increasingly viable as a miner's proportion of the hashrate grows. Conversely, under certain conditions, it has been shown that following the Bitcoin protocol is economically rational when the hashrate distribution is sufficiently decentralized [6].

To suppress excessive concentration of hashrate, it is crucial for mining to be fair. Here, we define mining fairness as the condition in which miners receive block rewards in proportion to the computational resources they commit. Unfairness in mining implies that certain miners receive greater rewards than others despite contributing proportionally similar computational effort. In particular, if miners with larger hashrates receive disproportionately higher block rewards—a phenomenon known as the Rich Get Richer (TRGR)—it suggests that the Bitcoin protocol inherently promotes hashrate centralization. For example, miners are incentivized to shift their hashrate from smaller mining pools to larger ones. This highlights a fundamental design flaw in Bitcoin.

In this study, we analyze the structure of TRGR in Bitcoin by investigating the impact of unintentional blockchain forks on mining fairness. Forks are an essential and unavoidable phenomenon in Bitcoin. Bitcoin was originally proposed as a highly decentralized system, in which miners act as independent agents and are geographically dispersed. As a result, Bitcoin functions as a distributed system, and its blockchain must be synchronized across the network whenever new blocks are generated. A blockchain fork occurs when a new block is generated before the previously mined block has been fully propagated throughout the network, making it an inherent part of the protocol's operation.

Although some prior work [7] has suggested the existence of TRGR, their analyses have relied on methods with insufficient accuracy. Specifically, the estimated impact of forks on mining fairness has been shown to deviate from actual values by more than 100% [8]. In this paper, we overcome this limitation by employing the model-based method proposed by Sakurai et al. [8], which significantly improves analytical accuracy by formally treating forks using time intervals called "rounds." This approach enables a precise assessment of the impact of forks on mining fairness.

Our main contributions in this study are as follows:

- *We theoretically demonstrate the existence of the Rich Get Richer (TRGR) phenomenon in Bitcoin under the assumption of fixed block propagation delays between different miners.* (Section VI)
  - We confirm that the mining profit rate increases monotonically and linearly with a miner's proportion of the total hashrate.
  - We mathematically establish the trade-off between decentralization and transaction processing capacity

through mining fairness. This result implies that improving block propagation delays can enhance mining fairness.
  - We demonstrate that the break-even point for mining profit rate increases as the hashrate distribution becomes more centralized. Specifically, we confirm that the break-even threshold is equal to the sum of the squares of the miners' hashrate proportions. This quantity increases as the distribution becomes more imbalanced. This implies that profitability becomes harder to achieve for all miners as the hashrate becomes more concentrated.
  - We show that the influence of the tie-breaking rule is relatively small compared to the effects of block propagation delay and block generation interval.
- We further validated and analyzed TRGR in Bitcoin when block propagation delays are not necessarily fixed. (Section VII)
  - By comparing the fixed-delay scenario with one where block propagation times are randomly distributed between different miners, we show that TRGR still holds on average. Furthermore, we demonstrate that the effect of propagation delay is more pronounced for small-scale miners with low hashrate.
  - Under a simplified setting in which miners can strategically adjust their block propagation delays, we showed that TRGR persists at Nash equilibrium.

II. Background

A. Bitcoin

In Bitcoin, users initiate transactions when they use the currency. These transactions are broadcast over the Bitcoin peer-to-peer (P2P) network and are grouped into blocks by nodes known as miners.

Each block references a single parent block, and this referencing structure forms a chain of blocks, known as the blockchain. Each miner maintains its own local view of blocks, and the longest chain is regarded as the valid transaction history, commonly referred to as the main chain.

To generate a block, a miner constructs a block template containing information such as the processed transactions, a timestamp, and the hash of the latest block on the main chain. The miner then performs repeated hash computations until the hash of the block header falls below a specified threshold. This process is known as mining. A block that satisfies this condition is considered valid and is propagated across the network. Upon verifying the block's validity, each miner updates its own main chain. Only blocks included in the main chain are considered valid transaction results, and the miner who generates such a block receives a block reward. This reward consists of a base reward and transaction fees.

An attacker invalidates a processed transaction by mining blocks that override the block containing the target transaction. Specifically, the attacker initiates a fork and constructs a new blockchain that is longer than the one in which the target transaction was included. To successfully carry out such an attack with certainty, the attacker would require computational power equivalent to the total network hashrate, which is generally considered prohibitively expensive and unrealistic. In this sense, the security of Bitcoin is ensured.

Even when all miners follow the Bitcoin protocol honestly, it is still possible for the blockchain to fork during block propagation. A fork occurs when a new block is generated by a miner before a previously mined block has been fully propagated throughout the network. The likelihood of a fork increases with block propagation delay [9]. In this study, we focus exclusively on such unintentional forks and do not consider intentional ones.

Each miner selects the longest blockchain as its main chain for mining. If there is ambiguity in identifying the longest chain due to a fork, a tie-breaking rule is used. In Bitcoin, the miner adopts the chain it received first—a policy known as the first-seen rule. This rule is used in practice due to its simplicity and effectiveness. However, from the perspective of selfish mining, it has a drawback: the overall security of the system becomes highly dependent on the attacker's block propagation capability [5]. To address this issue, alternative tie-breaking rules have been proposed, such as the random rule [5], which selects a chain at random, and the last-generated rule [10] [11] [12], which selects the chain containing the most recently generated block.

B. Mining Fairness

We define mining fairness as a state in which each miner receives block rewards in proportion to the computational resources (hashrate) they contribute to mining. Since blocks are generated in proportion to hashrate and the Bitcoin protocol adjusts mining difficulty to ensure that the total computational resources in the network match the rate of block generation, mining fairness holds as long as no forks occur. However, as discussed above, forks occur probabilistically, meaning not all blocks are included in the main chain. Consequently, some blocks receive no reward, and mining fairness is violated.

The impact of blockchain forks on mining fairness is influenced by several factors. The probability that a fork occurs depends on the block's propagation delay and the overall distribution of hashrate. For example, forks are less likely when propagation delays are short and the hashrate distribution is biased. Furthermore, whether a block involved in a fork is ultimately included in the main chain depends on factors such as the tie-breaking rule, propagation delay, and the block generator's proportion of the hashrate.

Understanding how forks affect mining fairness is not straightforward. For instance, a miner with a larger proportion of the hashrate is less likely to cause a fork when generating a block. However, this does not necessarily mean the miner will receive a larger reward. In selfish mining, the root cause of excessive block rewards for the attacker is the ability to invalidate blocks generated by honest miners. A miner with a large hashrate proportion has fewer opportunities to invalidate

others' blocks since their own blocks are less likely to result in forks. On the other hand, when a fork does occur, blocks generated by miners with a large hashrate proportion are more likely to be included in the main chain. This increases their expected block rewards and contributes to the TRGR effect.

The aim of this study is to analyze the impact of unintentional blockchain forks on mining fairness and to determine whether TRGR holds in Bitcoin. To ensure decentralization, Bitcoin relies on independent miners that are geographically distributed. In such a system, blockchain forks are unavoidable due to block propagation delays.

While other factors may also affect mining fairness—such as ASIC performance or electricity costs—these are not considered in this study, as their influence is comparatively straightforward to understand.

III. Related Work

Chen et al. examined the impact of unintentional blockchain forks on mining fairness in Bitcoin [7]. One of their conclusions is that TRGR phenomenon holds in Bitcoin. However, their analytical method suffers from low precision and limited generality. Specifically, they did not consider the effect of forks on the rate at which miners initiate new rounds, nor the increase in block rewards due to fork creation. According to the study by Sakurai et al. [8], neglecting the effect of forks on the proportion of round initiation alone can result in over 100% error in estimating actual mining fairness.

Attacks that intentionally exploit forks—such as selfish mining [5], fork-after-withholding [13]—also suggest the existence of TRGR in Bitcoin. For instance, in selfish mining, the attacker's block reward increases with the attacker's hashrate proportion. Further studies that incorporate the effect of stale blocks into selfish mining [14], [15] suggest that longer block propagation times intensify the TRGR effect.

We now turn to studies that investigate TRGR in terms of hashrate distribution, without considering forks. Judmayer et al. showed that a small number of mining pools control the majority of the network's hashrate by attributing each block to its generator pool [16]. Romiti et al. refined this attribution method to improve accuracy and demonstrated, using the Gini coefficient, that the hashrate distribution is highly concentrated [17]. Cong et al. argued that large mining pools do not necessarily grow further, since individual miners can split their hashrate across multiple pools and large pools tend to impose higher fees [18]. Huang et al. investigated whether TRGR arises in blockchain systems [19]. They primarily showed that TRGR appears in Proof-of-Stake-based systems, but concluded that it does not occur in Proof-of-Work systems. This conclusion, however, stems from their failure to account for the impact of blockchain forks. Li et al. argued, using a mean-field game model, that reward instability itself can give rise to TRGR [20].

Next, we review studies that analyze TRGR from the perspective of wealth distribution. Ron et al. examined transaction data on the blockchain and found that wealth distribution in Bitcoin is extremely skewed [21]. They also identified that a significant proportion of Bitcoin's transaction volume originates from a single transaction issued in 2010. From a network science perspective, Kondor et al. demonstrated signs of TRGR by analyzing transaction histories [22], [23]. Similar trends were also confirmed by Gupta et al. [24], Maesa et al. [25], and Venturini et al. [26]. Sai et al. examined multiple cryptocurrency systems and found that while systems with large market capitalizations tend to be relatively more decentralized, wealth concentration remains [27]. Juodis et al. extended the analysis to Layer-2 cryptocurrency systems and introduced the Herfindahl–Hirschman Index (HHI) as a metric [28]. Kusmiers et al. compared ERC-20 tokens [29] with Bitcoin and showed that ERC-20 tokens tend to exhibit higher centralization [30].

IV. Model

We describe the Bitcoin network model used in this study, following Sakurai et al. [8]. We assume that all miners are honest and follow the Bitcoin protocol. The set of miners is denoted by V, which is fixed throughout the analysis. Each miner $i \in V$ is assigned a hashrate proportion α_i, satisfying $\sum_{i \in V} \alpha_i = 1$. We assume that at most two blocks can be generated per round. A round is defined as a global time interval, specifically, the period between the generation of the first block at height r and the generation of the first block at height $r + 1$. This round-based model of the blockchain network enables us to formally handle forks and precisely capture their impact on mining fairness.

A fork is defined as the event in which two blocks are generated within a single round. Let F_{ij} denote the probability that a fork occurs when miner i initiates a round and subsequently miner j generates a block. Let W_{ij} denote the probability that, in such a fork, the block generated by miner i is included in the main chain. We assume that the block reward is a fixed value across all blocks.

V. Method for Calculating Mining Profit Rate

In this study, we use the mining profit rate as an indicator to analyze mining fairness. Mining profit rate refers to the mining profit earned per unit of computational resource. In this section, we explain the method proposed by Sakurai et al. [8] for calculating mining profit rate. Their method performs this calculation within a round-based blockchain network model, providing a high-speed and accurate alternative to simulation-based approaches. Simulation results have verified that this method significantly improves the accuracy of mining fairness analysis compared to existing techniques.

The parameters required to compute the mining profit rate are: the hashrate proportion α_i of each miner i, the block propagation delay T_{ij} from miner i to miner j, and the average block generation interval T. The propagation delay T_{ij} is defined as the time it takes for a block generated by miner i to reach miner j.

We first calculate the fork rate F_{ij}, which is the probability that miner j causes a fork in the same round under the condition that miner i initiates the round and miner j is the next to

generate a block. In blockchain networks, block generation intervals follow an exponential distribution. Therefore, the probability that the next block is generated before the previous one reaches other miners corresponds to the fork probability, and is given by:

$$F_{ij} = 1 - \exp\left(-\frac{T_{ij}}{T}\right) \tag{1}$$

Next, we compute the probability W_{ij} that miner i's block is included in the main chain when a fork occurs between miners i and j. This probability can be approximately calculated based on the tie-breaking rule, the hashrate distribution, and the propagation delay. For details of the approximation method, we refer the reader to the study by Sakurai et al. [8].

We then compute the proportion of round initiation for each miner. The proportion of round initiation of a miner is the probability that the miner generates the block that starts a new round—equivalently, the probability that the blockchain height is updated by that miner. Let X_r be the random variable representing the miner who initiates round r. Then, the following recurrence holds:

$$P(X_{r+1} = i) = \sum_{j \in V} \left(\alpha_i (1 - F_{ji}) + \sum_{k \in V} \alpha_k F_{jk} \alpha_i \right) P(X_r = j) \tag{2}$$

Since this process forms an ergodic Markov chain, its limit distribution converges to a stationary distribution. By iterating the above equation, we can obtain the proportion of round initiation π_i for each miner i.

Once π_i is computed, the proportion of block reward r_i for miner i is given by:

$$\begin{aligned} r_i =& \pi_i \left(1 - \sum_{j \in V} \alpha_j F_{ij} + \sum_{j \in V} \alpha_j F_{ij} W_{ij} \right) \\ &+ \sum_{j \in V} \pi_j \alpha_i F_{ji} (1 - W_{ji}) \end{aligned} \tag{3}$$

From the proportion of block reward, we can compute the mining profit MP_i and mining profit rate MPR_i for miner i as follows:

$$MP_i = r_i - \alpha_i \tag{4}$$

$$MPR_i = \frac{MP_i}{\alpha_i} \tag{5}$$

In Bitcoin, the block generation difficulty is adjusted approximately every two weeks. This adjustment ensures that the total computational effort spent on mining matches the total rewards distributed. As a result, by comparing a miner's hashrate proportion α_i with its proportion of block reward r_i, we can evaluate the mining profit and mining profit rate of that miner.

VI. Fixed Block Propagation Delay Between Different Miners

We analyze the structure of the TRGR effect in Bitcoin under the condition that block propagation delays between different miners are fixed. First, in Section VI-A, we derive an approximate theoretical formula for mining profit rate. Next, in Section VI-B, we verify this formula through numerical computation. Finally, we discuss the insights obtained from the derived approximation in Section VI-C.

A. Theoretical Analysis

We perform a theoretical analysis that does not rely on specific parameter values.

The block propagation delay between any two distinct miners is fixed at d. We assume that the ratio d/T between the propagation delay d and the average block generation interval T is sufficiently small. Under these conditions, the fork rate F_{ij} is given by:

$$F_{ij} = \begin{cases} 0 & \text{if } i = j, \\ 1 - \exp(-\frac{d}{T}) & \text{if } i \neq j. \end{cases} \tag{6}$$

Hereafter, we denote F_{ij} by f for $i \neq j$. Since $f \approx d/T$, we can treat f as a sufficiently small parameter.

We first compute the proportion of round initiation π_i for miner i. From Equation 2, we obtain:

$$\pi_i = \sum_{j \in V} \left(\alpha_i (1 - F_{ji}) + \sum_{k \in V} \alpha_k F_{jk} \alpha_i \right) \pi_j \tag{7}$$

$$= \alpha_i + \alpha_i f (\alpha_i - \sum_{j \in V} \alpha_j \pi_j) \tag{8}$$

By substituting $\pi_j = \alpha_j$ on the right-hand side for all j, we get:

$$\pi_i \approx \alpha_i + \alpha_i f (\pi_i - \sum_{j \in V} \alpha_j^2) \tag{9}$$

This gives an approximate expression for the proportion of round initiation of each miner i. Notably, this result is independent of the tie-breaking rule.

Recalling that the block propagation delay between different miners is fixed, the value of W_{ij} depends on the tie-breaking rule and is given by:

$$W_{ij} = \begin{cases} 1 - \alpha_j & \text{first-seen rule,} \\ \frac{1 - \alpha_j + \alpha_i}{2} & \text{random rule,} \\ \alpha_i & \text{last-generated rule.} \end{cases} \tag{10}$$

For instance, under the first-seen rule, the block that initiates the round reaches all miners other than miner j before the forked block, so these miners mine on the block generated by miner i.

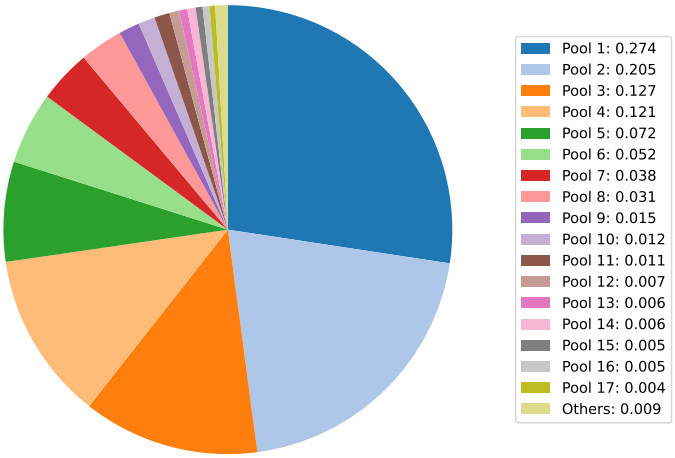


Fig. 1: Hashrate distribution in Bitcoin.

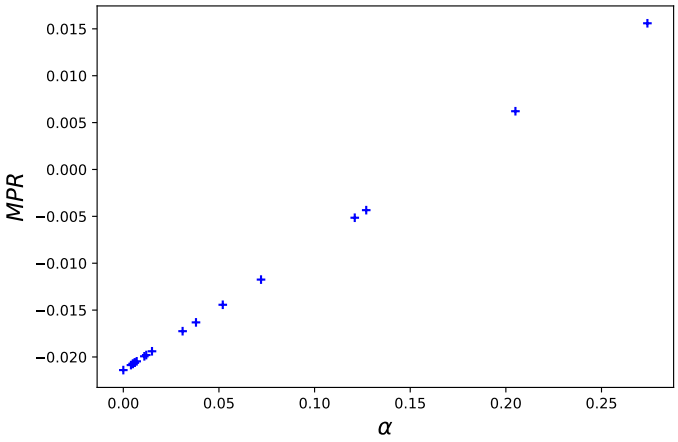


Fig. 2: Numerical results for mining profit rate.

Next, we calculate the proportion of block reward r_i for miner i. From Equation 3, we obtain:

$$r_i = \pi_i \left(1 - \sum_{j \in V} \alpha_j F_{ij} + \sum_{j \in V} \alpha_j F_{ij} W_{ij}\right) + \sum_{j \in V} \pi_j \alpha_i F_{ji} (1 - W_{ji}) \tag{11}$$

$$= \alpha_i + 2\alpha_i f(\alpha_i - \sum_{j \in V} \alpha_j^2) + \mathcal{O}(f^2) \tag{12}$$

$$\approx \alpha_i + 2\alpha_i f(\alpha_i - \sum_{j \in V} \alpha_j^2) \tag{13}$$

Therefore,

$$r_i = \alpha_i + 2\alpha_i f(\alpha_i - \sum_{j \in V} \alpha_j^2) \tag{14}$$

$$\iff MPR_i = \frac{r_i - \alpha_i}{\alpha_i} = 2f(\alpha_i - \sum_{j \in V} \alpha_j^2) \tag{15}$$

The approximation in Equation 15 is justified by the assumption that f is sufficiently small. Moreover, this result does not depend on the tie-breaking rule.

B. Validation via Numerical Computation

In the preceding analysis, two approximations were employed, specifically those in Equations 9 and 15. Here, we verify the validity of these approximations. Concretely, we substitute actual parameter values used in the method by Sakurai et al. [31] and compare the numerical results with those obtained from our theoretical analysis. If the numerical results agree with the theoretical ones, and considering that these numerical results closely reflect the actual values observed in Bitcoin, we can conclude that our theoretical analysis is applicable to Bitcoin.

The specific parameters used were as follows: the number of miners was set to 1000, the average block generation interval was $T = 600$, and the hashrate distribution was based on the actual distribution observed in Bitcoin [31] (see Figure 1). To be precise, hashrates were assigned to miners to match the distribution shown in the figure, and the remaining hash power was evenly distributed among the rest of the miners. We considered three tie-breaking rules: the first-seen rule, the random rule, and the last-generated rule.

For the block propagation delay d between different miners, we considered values up to 42. This choice was motivated by three reasons. First, from the nature of the approximation, the smaller the block propagation delay between different miners, the more accurate the approximation becomes. Thus, our theoretical result remains applicable for $d \leq 42$. Second, the ratio d/T is lower than those found in most blockchain systems, including Ethereum, which has a small block interval (approximately $d/T = 0.7$ [14]) [32]. Lastly, Sakurai et al.'s method has been validated using simulations for values of d/T up to 0.1.

Figure 2 presents the numerical results for the mining profit rate MPR_i under the first-seen rule. As in Equation 15, the results demonstrate that MPR_i depends linearly on the miner's proportion of the total hashrate. The average correlation coefficient across the three tie-breaking rules is 0.999992, indicating that this linear dependency holds irrespective of the choice of tie-breaking rule.

A line is determined by its slope and a point on the line. We first compare the slopes. Table I presents the theoretically derived slope $2f$ alongside the results from numerical computation under the first-seen rule. The theoretical slope closely matches the numerical one.

Next, we compare the zero-point of the mining profit rate. Since MPR_i is linearly dependent on α_i, the following holds:

$$MPR_i = k(\alpha_i - \alpha_0), \tag{16}$$

where k is the slope of the line, α_i denotes the hashrate proportion of miner i, and α_0 denotes the zero-point. We now demonstrate that this zero-point equals $\sum \alpha_i^2$. From Equation 16, we obtain:

$$MPR_i \alpha_i = \alpha_i k(\alpha_i - \alpha_0), \tag{17}$$

$$\iff MP_i = k\alpha_i^2 - k\alpha_0\alpha_i. \tag{18}$$

TABLE I: Comparison of theoretical and numerical slopes.

d/T	Theoretical result	Numerical result
0.01	0.0199003	0.019896
0.04	0.0784211	0.0783533
0.07	0.135212	0.135011

Summing over all miners yields:

$$\sum_{i\in V} MPR_i = \sum_{i\in V} \left(k\alpha_i^2 - k\alpha_0\alpha_i\right) \tag{19}$$

$$\iff 0 = k\sum_{i\in V} \alpha_i^2 - k\alpha_0 \sum_{i\in V} \alpha_i \tag{20}$$

$$\iff \alpha_0 = \sum_{i\in V} \alpha_i^2. \tag{21}$$

Thus, the zero-point of the mining profit rate in numerical results equals $\sum \alpha_i^2$.

In summary, we have confirmed that the results from the theoretical analysis agree with those obtained through numerical calculation. This supports the conclusion that our theoretical analysis is applicable to the actual Bitcoin network.

C. Insights

Equation 15 offers several important insights. In this section, we elaborate on each of them in detail.

First, regarding whether the TRGR, the central focus of this study, holds in Bitcoin: we find that it does hold in the sense that a higher hashrate proportion leads to a higher mining profit rate. In particular, the mining profit rate depends linearly on the hashrate proportion.

Second, Equation 15 clarifies the trade-off between Bitcoin's transaction processing capacity and its degree of decentralization (Figure 3). Focusing on the slope of 15, we see that it is $2f$, where f is defined as $1 - \exp(-d/T)$. In other words, f increases with greater block propagation delay d or shorter block generation interval T. Since larger block sizes increase propagation delay, f tends to increase as the system's transaction processing capacity increases. An increase in f signifies a stronger TRGR tendency, thus undermining decentralization.

Next, we consider the impact of hashrate distribution. Equation 15 shows that the zero-crossing point of the mining profit rate is equal to the sum of the squares of the hashrate proportions. This value increases when the hashrate distribution becomes more skewed, indicating that the mining efficiency of the system decreases as the distribution becomes more centralized.

We then consider the effect of the tie-breaking rule. At first glance, Equation 15 seems to suggest that the tie-breaking rule has no effect on the mining profit rate. However, Sakurai et al.'s block reward formula 3 suggests that the last-generated rule contributes the most to improving fairness, while the first-seen rule degrades it the most. This discrepancy arises because, in deriving 15, a term with coefficient f^2—which contains the influence of the tie-breaking rule—was approximated away.

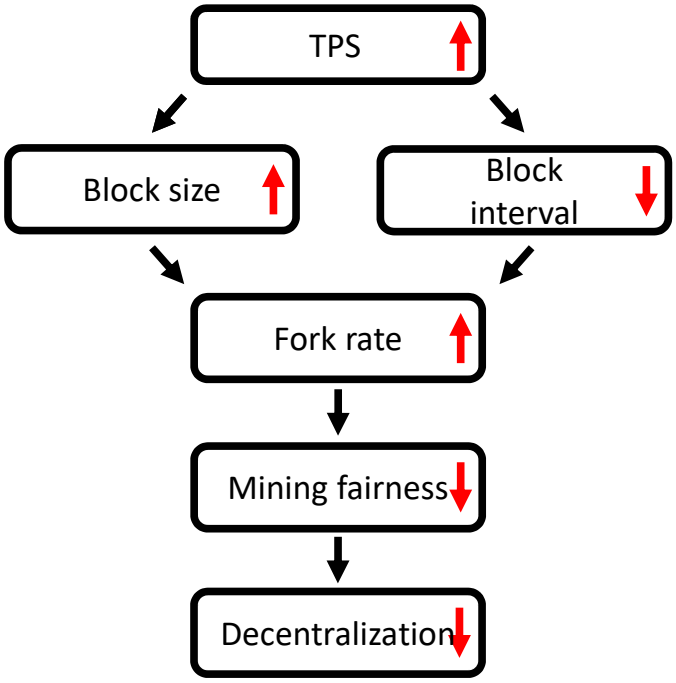


Fig. 3: The trade-off between transaction processing capacity and decentralization. Increasing the block size or shortening the block interval improves transaction throughput, but also leads to more frequent blockchain forks. While more forks do not necessarily imply a stronger TRGR and thus may not always reduce decentralization, Equation 15 clearly shows that improving throughput inherently strengthens TRGR, and consequently undermines decentralization.

Thus, the effect of the tie-breaking rule is embedded in the term that was neglected. Conversely, this also implies that in systems with larger f, the mining profit rate is more sensitive to the choice of tie-breaking rule.

VII. Variable Block Propagation Delays Between Different Miners

The previous analyses were conducted under the assumption that block propagation delays between different miners are fixed. In this section, we investigate the robustness of those results under conditions where this assumption does not necessarily hold. Specifically, we first compare the cases where block propagation delays are fixed and where they are randomized. Then, from the perspective of economic rationality, we examine whether TRGR is preserved when miners are allowed to strategically manipulate block propagation delays.

A. Randomizing Block Propagation Delays

We compare the cases with randomized and fixed block propagation delays to examine how the structure of TRGR changes under randomness.

1) Model of the Block Propagation Protocol: In Bitcoin, blocks are propagated via a gossip-based flooding protocol, meaning that each miner forwards blocks to its neighbors. Under this protocol, the dissemination of a block throughout

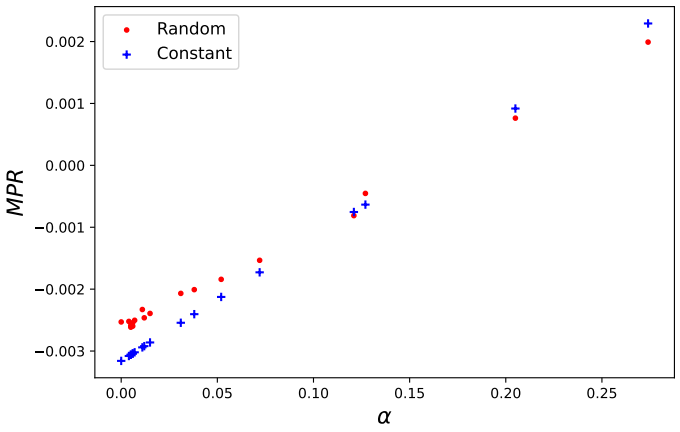


Fig. 4: Comparison of the average mining profit rate between the case where block propagation delays between miners are randomized and the case where they are fixed.

the system is commonly modeled using the following logistic differential equation:

$$\frac{dI}{dt} = \beta I(N - I), \tag{22}$$

where β is a constant, $I(t)$ denotes the number of miners that have received the block by time t, and N is the total number of miners.

Under the initial condition $I(0) = 1$, the solution of this equation is given by:

$$I(t) = \frac{N}{1 + (N-1)\exp^{-\beta N t}}. \tag{23}$$

Considering $I(t)/N$ as the cumulative distribution function (CDF) of a probability distribution, this corresponds to a logistic distribution. Therefore, the expected value of the block propagation delay is given by $\ln(N-1)/(\beta N)$.

2) Settings: We set the number of miners to $N = 1000$ and the average block generation interval to $T = 600$ seconds. The distribution of hashrates among miners was based on the actual distribution observed in Bitcoin (see Figure 1).

Block propagation delays between miners were randomly drawn from a logistic distribution with a mean of 6.

3) Results: We conducted 100 simulations of mining profit rates under randomized block propagation delays between miners. Figure 4 shows the comparison of the results with those from the fixed-delay setting. The figure suggests that the average values are approximately the same in both cases. This is likely because F_{ij}, which depends on T_{ij}/T, can be approximated linearly with respect to T_{ij} when T_{ij}/T is sufficiently small.

Figure 5 shows the standard deviation of each miner's mining profit rate under the randomized setting. As seen in the figure, miners with smaller proportions of hashrate tend to exhibit higher standard deviation in their mining profit rates. This indicates that smaller miners are more susceptible to fluctuations in block propagation delays.

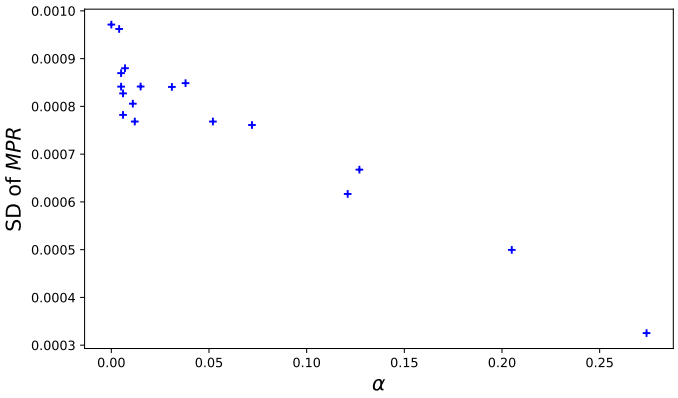


Fig. 5: Standard deviation of mining profit rates under randomized block propagation delays between miners.

B. From the Perspective of Economic Rationality

We investigate whether TRGR is preserved under variable block propagation delays from the perspective of economic rationality. More specifically, we analyze the case under the assumption that each miner is allowed to manipulate block propagation delays as part of their strategy to maximize their own mining profit rate.

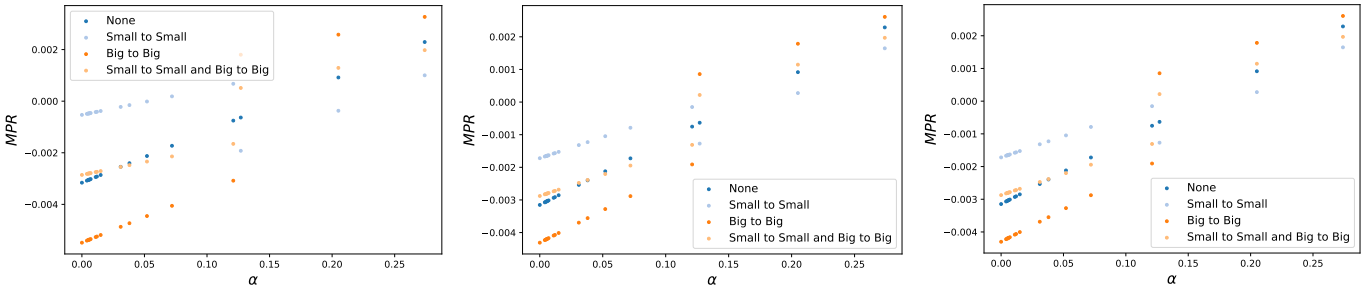
1) Setup: We considered $N = 1000$ miners and set the average block generation interval to $T = 600$ seconds. The hashrate distribution was based on the actual distribution observed in the Bitcoin network (see Figure 1).

It is not easy to analyze the full strategy space of all miners. Therefore, we simplified the setting as follows. Each miner's strategy consists of choosing the propagation delay for blocks it sends. The block propagation delay between any pair of miners was set to either $d = 3$ (fast propagation) or $d = 6$ (slow propagation). We assumed that all miners were equally capable of accelerating or delaying propagation. In practice, selecting between fast and slow propagation is relatively easy. To slow propagation, a miner can delay transmission or continue mining as if it has not received the block. To accelerate propagation, a miner can establish a direct connection or use high-bandwidth modes such as Compact Block Relay [33].

Miners were divided into two groups: large and small miners. Specifically, the group of miners accounting for the top 50% of the total hashrate was defined as large miners. All miners within each group were treated homogeneously. For example, if one large miner chooses to propagate blocks quickly to another large miner, then all large miners are assumed to do the same toward all other large miners.

The utility of each group was defined as the aggregated mining profit rate of the miners in that group.

2) Results: First, we observe that fast block propagation from large miners to small miners, or vice versa, is not a rational outcome. This is because accelerating block propagation requires agreement from both the sender and the receiver, and Bitcoin mining is a zero-sum game. If a large miner propagates a block faster to a small miner and gains a profit, the small miner must lose an equivalent amount. In this case,



(a) First-seen rule. (b) Random rule. (c) Last-generated rule.

Fig. 6: Numerical results of the strategic interactions.

small miners have no incentive to cooperate in accelerating propagation, and mutual agreement cannot be established.

From this reasoning, the only viable strategies for large miners are whether to propagate blocks quickly to other large miners. Similarly, small miners can only decide whether to accelerate propagation to other small miners.

Figure 6 shows the outcomes of each group's strategies. The results indicate that accelerating block propagation within one's own group improves that group's mining profit rate. Furthermore, a Nash equilibrium is reached when both groups choose to accelerate block propagation within their own group. In this equilibrium, the TRGR structure remains intact, indicating that the emergence of TRGR is consistent with economic rationality.

VIII. Discussion

A. Mitigating TRGR

In this section, we discuss potential approaches to mitigating TRGR.

One straightforward approach is to reduce block propagation delays. As suggested by Eq. 15, reducing block propagation delays leads to a smaller slope, thereby improving the overall mining fairness of the system. A key advantage of this approach is its compatibility with the existing system. Improvements to block propagation protocols can be implemented without requiring changes to the Bitcoin protocol itself [34], [35]. Such compatibility is especially important for Bitcoin, which is a currency system and favors conservative system operations. On the other hand, implementing these propagation protocols is not a fully local operation; it requires coordination between communication peers.

Another promising approach is to modify the tie-breaking rule. Among the possible options, the first-seen rule leads to the most unfair outcomes. Because Bitcoin is a decentralized system, miners with higher hashrates tend to have a higher proportion of round initiation. Under the first-seen rule, miners who initiate rounds more frequently gain an advantage in tie situations, amplifying the inequality. In contrast, the random rule and the last-generated rule help suppress disparities in proportions of round initiation and thereby improve mining fairness.

Compared to the propagation delay improvement approach, modifying the tie-breaking rule has the benefit of better local compatibility. For instance, the method proposed by Sakurai et al. [10] can be implemented and operated entirely locally by each miner. However, as indicated by Eq. 15, the impact of modifying the tie-breaking rule on mining fairness is generally smaller than that of improving block propagation delays.

A third approach is to reward stale blocks—i.e., blocks that are not included in the main chain. In principle, since each miner's number of generated blocks aligns with its hashrate proportion, this mechanism can achieve mining fairness. Similar approaches have been proposed in prior studies to counter attacks that degrade mining fairness [5], [36], [37]. However, this approach has two major drawbacks. The first is compatibility with Bitcoin. As a currency system, Bitcoin tends to favor conservative upgrades. Most existing proposals for rewarding stale blocks break backward compatibility, making them difficult to deploy in practice. There are more compatible alternatives, such as decentralized mining pools [38]–[40], but research into incentive mechanisms for participating in such pools is still limited, and it remains unclear how widely these systems can be adopted.

The second issue is that rewarding stale blocks may increase the incentive to attack the Bitcoin network. If forked blocks receive rewards, then blocks intentionally generated for attacks would also be rewarded. Indeed, prior research [41] has shown that Ethereum [42], which partially adopts this approach, faces an increased risk of selfish mining as a result.

B. The Importance of Considering Proportions of Round Initiation in Mining Fairness Analysis

Simulation experiments have shown that neglecting the effect of forks on proportions of round initiation can lead to mining profit estimation errors of nearly 100% [8]. The high accuracy of Sakurai et al.'s method stems mainly from the fact that their blockchain model is round-based, allowing forks to be treated formally. However, it was previously unclear why ignoring the influence of forks on proportions of round initiation causes such large errors.

To clarify this, we compute the mining profit rate under the assumption that proportions of round initiation are equal

to hashrate proportions, i.e., ignoring the impact of forks. By proceeding with calculations as in Section VI-A, we obtain:

$$MPR_i = f\left(\alpha_i - \sum_{j \in V} \alpha_j^2\right). \tag{24}$$

In contrast, when considering the impact of forks on proportions of round initiation, the profit rate becomes:

$$MPR_i = 2f\left(\alpha_i - \sum_{j \in V} \alpha_j^2\right). \tag{25}$$

This result shows that the effect of forks on proportions of round initiation is as significant as their other effects on mining fairness.

C. Limitations

The simplified form of TRGR, as expressed in Eq. 15, is derived under the assumption of fixed block propagation delays. While we have shown that TRGR still holds under economic rationality even when delays are variable, the setting used in this analysis is deliberately limited to ensure tractability. For example, we grouped miners into two categories—those accounting for the top 50% of total hashrate and others—and treated all miners within each group identically. Investigating how far such assumptions can be relaxed while preserving TRGR is an important direction for future work.

In addition, our study neglects the distributed nature of mining pools. Although mining pools behave like single miners on the Bitcoin network, they are in fact composed of multiple cooperating miners who are geographically distributed. Due to this distributed nature, discarded blocks that are not recorded on the blockchain may still be generated, which could affect mining fairness.

However, we argue that the effect of intra-pool distribution can be ignored. During synchronization within a pool, each miner only receives minimal information necessary for mining from the pool server. This data is significantly smaller than what is needed to participate in the Bitcoin network itself, so synchronization within the pool is fast. Therefore, the impact of intra-pool delays is expected to be much smaller than inter-miner delays on the public network.

IX. Conclusion

In this study, we theoretically demonstrate TRGR in Bitcoin under the assumption of fixed block propagation delays between miners, using a significantly more precise method than previous research. We also analyze the impact of block propagation delay, hashrate, and the tie-breaking rule on TRGR. Furthermore, we validate TRGR in a setting where block propagation delays are not fixed.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[2] J. Garay, A. Kiayias, and N. Leonardos, "The bitcoin backbone protocol: Analysis and applications," in *Advances in Cryptology - EUROCRYPT 2015*, E. Oswald and M. Fischlin, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 281–310.

[3] A. Dembo, S. Kannan, E. N. Tas, D. Tse, P. Viswanath, X. Wang, and O. Zeitouni, "Everything is a race and nakamoto always wins," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '20. New York, NY, USA: Association for Computing Machinery, 2020, p. 859–878. [Online]. Available: https://doi.org/10.1145/3372297.3417290

[4] P. Gaži, A. Kiayias, and A. Russell, "Tight consistency bounds for bitcoin," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '20. New York, NY, USA: Association for Computing Machinery, 2020, p. 819–838. [Online]. Available: https://doi.org/10.1145/3372297.3423365

[5] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in *Financial Cryptography and Data Security*, N. Christin and R. Safavi-Naini, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 436–454.

[6] A. Kiayias, E. Koutsoupias, M. Kyropoulou, and Y. Tselekounis, "Blockchain mining games," in *Proceedings of the 2016 ACM Conference on Economics and Computation*, ser. EC '16. New York, NY, USA: Association for Computing Machinery, 2016, p. 365–382. [Online]. Available: https://doi.org/10.1145/2940716.2940773

[7] C. Chen, X. Chen, J. Yu, W. Wu, and D. Wu, "Impact of temporary fork on the evolution of mining pools in blockchain networks: An evolutionary game analysis," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 1, pp. 400–418, 2021.

[8] A. Sakurai and K. Shudo, "Model-based analysis of mining fairness in a blockchain," 2025, arXiv: 2406.00595. [Online]. Available: https://arxiv.org/abs/2406.00595

[9] C. Decker and R. Wattenhofer, "Information propagation in the bitcoin network," in *IEEE P2P 2013 Proceedings*, 2013, pp. 1–10.

[10] A. Sakurai and K. Shudo, "A fully local last-generated rule in a blockchain," 2024, arXiv: 2411.08439. [Online]. Available: https://arxiv.org/abs/2411.08439

[11] A. Sakurai and K. Shudo, "Tie-breaking rule based on partial proof of work in a blockchain," *IEEE Access*, vol. 12, pp. 197 999–198 014, 2024.

[12] E. Heilman, "One weird trick to stop selfish miners: Fresh bitcoins, a solution for the honest miner (poster abstract)," in *Financial Cryptography and Data Security*, R. Böhme, M. Brenner, T. Moore, and M. Smith, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 161–162.

[13] Y. Kwon, D. Kim, Y. Son, E. Vasserman, and Y. Kim, "Be selfish and avoid dilemmas: Fork after withholding (faw) attacks on bitcoin," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '17. New York, NY, USA: Association for Computing Machinery, 2017, p. 195–209. [Online]. Available: https://doi.org/10.1145/3133956.3134019

[14] 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 *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '16. New York, NY, USA: Association for Computing Machinery, 2016, p. 3–16. [Online]. Available: https://doi.org/10.1145/2976749.2978341

[15] C. Schwarz-Schilling, S.-N. Li, and C. J. Tessone, "Stochastic modelling of selfish mining in proof-of-work protocols," *Journal of Cybersecurity and Privacy*, vol. 2, no. 2, pp. 292–310, 2022. [Online]. Available: https://www.mdpi.com/2624-800X/2/2/16

[16] A. Judmayer, A. Zamyatin, N. Stifter, A. G. Voyiatzis, and E. Weippl, "Merged mining: Curse or cure?" in *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, J. Garcia-Alfaro, G. Navarro-Arribas, H. Hartenstein, and J. Herrera-Joancomartí, Eds. Cham: Springer International Publishing, 2017, pp. 316–333.

[17] M. Romiti, A. Judmayer, A. Zamyatin, and B. Haslhofer, "A deep dive into bitcoin mining pools: An empirical analysis of mining shares," in *Workshop on the Economics of Information Security (WEIS)*, Boston, MA, 2019, june 3–4, 2019. [Online]. Available: https://weis2019.econinfosec.org/program/agenda/

[18] L. W. Cong, Z. He, and J. Li, "Decentralized mining in centralized pools," *The Review of Financial Studies*, vol. 34, no. 3, pp. 1191–1235, 04 2020. [Online]. Available: https://doi.org/10.1093/rfs/hhaa040

[19] Y. Huang, J. Tang, Q. Cong, A. Lim, and J. Xu, "Do the rich get richer? fairness analysis for blockchain incentives," in *Proceedings of the 2021 International Conference on Management of Data*, ser. SIGMOD '21. New York, NY, USA: Association for Computing Machinery, 2021, pp. 790–803. [Online]. Available: https://doi.org/10.1145/3448016.3457285

[20] Z. Li, A. M. Reppen, and R. Sircar, "A mean field games model for cryptocurrency mining," *Management Science*, vol. 70, no. 4, pp. 2188–2208, 2024. [Online]. Available: https://doi.org/10.1287/mnsc.2023.4798

[21] D. Ron and A. Shamir, "Quantitative analysis of the full bitcoin transaction graph," in *Financial Cryptography and Data Security*, A.-R. Sadeghi, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 6–24.

[22] D. Kondor, M. Pósfai, I. Csabai, and G. Vattay, "Do the rich get richer? an empirical analysis of the bitcoin transaction network," *PLOS ONE*, vol. 9, no. 2, pp. 1–10, 02 2014. [Online]. Available: https://doi.org/10.1371/journal.pone.0086197

[23] D. Kondor, N. Bulatovic, J. Stéger, I. Csabai, and G. Vattay, "The rich still get richer: Empirical comparison of preferential attachment via linking statistics in bitcoin and ethereum," *Frontiers in Blockchain*, vol. Volume 4 - 2021, 2021. [Online]. Available: https://www.frontiersin.org/journals/blockchain/articles/10.3389/fbloc.2021.668510

[24] M. Gupta and P. Gupta, "Gini coefficient based wealth distribution in the bitcoin network: A case study," in *Computing, Analytics and Networks*, R. Sharma, A. Mantri, and S. Dua, Eds. Singapore: Springer Singapore, 2018, pp. 192–202.

[25] D. Di Francesco Maesa, A. Marino, and L. Ricci, "Data-driven analysis of bitcoin properties: exploiting the users graph," *International Journal of Data Science and Analytics*, vol. 6, no. 1, pp. 63–80, Aug. 2018. [Online]. Available: https://doi.org/10.1007/s41060-017-0074-x

[26] M. Venturini, D. García-Costa, E. Álvarez García, F. Grimaldo, and F. Squazzoni, "Mapping network structures and dynamics of decentralised cryptocurrencies: The evolution of bitcoin (2009-2023)," 2025. [Online]. Available: https://arxiv.org/abs/2501.11416

[27] A. R. Sai, J. Buckley, and A. Le Gear, "Characterizing wealth inequality in cryptocurrencies," *Frontiers in Blockchain*, vol. Volume 4 - 2021, 2021. [Online]. Available: https://www.frontiersin.org/journals/blockchain/articles/10.3389/fbloc.2021.730122

[28] M. Juodis, E. Filatovas, and R. Paulavičius, "Overview and empirical analysis of wealth decentralization in blockchain networks," *ICT Express*, vol. 10, no. 2, pp. 380–386, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2405959524000079

[29] F. Vogelsteller and V. Buterin, "ERC-20: Token Standard," https://eips.ethereum.org/EIPS/eip-20, 2015, ethereum Improvement Proposal.

[30] B. Kusmierz and R. Overko, " How centralized is decentralized? Comparison of wealth distribution in coins and tokens ," in *2022 IEEE International Conference on Omni-layer Intelligent Systems (COINS)*. Los Alamitos, CA, USA: IEEE Computer Society, Aug. 2022, pp. 1–6. [Online]. Available: https://doi.ieeecomputersociety.org/10.1109/COINS54846.2022.9854972

[31] "Mining pool stats," Online, 2025, accessed: 2025-05-19. [Online]. Available: https://miningpoolstats.stream/

[32] J. Fechner, B. Chandrasekaran, and M. X. Makkes, "Calibrating the performance and security of blockchains via information propagation delays: revisiting an old approach with a new perspective," in *Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing*, ser. SAC '22. New York, NY, USA: Association for Computing Machinery, 2022, pp. 282–289. [Online]. Available: https://doi.org/10.1145/3477314.3507003

[33] M. Corallo, "Compact block relay," https://github.com/bitcoin/bips/blob/master/bip-0152.mediawiki, 2016, accessed: Aug. 16. 2022.

[34] D. A. Harding and P. Todd, "Bip 0125: Opt-in full replace-by-fee signaling," https://github.com/bitcoin/bips/blob/master/bip-0125.mediawiki, 2016, accessed: 2023-8-23.

[35] 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 *Proceedings of the ACM Special Interest Group on Data Communication*, ser. SIGCOMM '19. New York, NY, USA: Association for Computing Machinery, 2019, pp. 303–317. [Online]. Available: https://doi.org/10.1145/3341302.3342082

[36] R. Pass and E. Shi, "Fruitchains: A fair blockchain," in *Proceedings of the ACM Symposium on Principles of Distributed Computing*, ser. PODC '17. New York, NY, USA: Association for Computing Machinery, 2017, p. 315–324. [Online]. Available: https://doi.org/10.1145/3087801.3087809

[37] V. Bagaria, S. Kannan, D. Tse, G. Fanti, and P. Viswanath, "Prism: Deconstructing the blockchain to approach physical limits," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '19. New York, NY, USA: Association for Computing Machinery, 2019, pp. 585–602. [Online]. Available: https://doi.org/10.1145/3319535.3363213

[38] "P2Pool - decentralized bitcoin mining pool," http://p2pool.in/, 2024, accessed: 2024-04-27.

[39] L. Luu, Y. Velner, J. Teutsch, and P. Saxena, "SmartPool: Practical decentralized pooled mining," in *26th USENIX Security Symposium (USENIX Security 17)*. Vancouver, BC: USENIX Association, Aug. 2017, pp. 1409–1426. [Online]. Available: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/luu

[40] A. Sakurai and K. Shudo, "Fiberpool: Leveraging multiple blockchains for decentralized pooled mining," 2025, arXiv: 2501.15459. [Online]. Available: https://arxiv.org/abs/2501.15459

[41] Y. Liu, Y. Hei, T. Xu, and J. Liu, "An evaluation of uncle block mechanism effect on ethereum selfish and stubborn mining combined with an eclipse attack," *IEEE Access*, vol. 8, pp. 17 489–17 499, 2020.

[42] "Ethereum: A secure decentralised generalised transaction ledger," https://ethereum.github.io/yellowpaper/paper.pdf.