Selfish Mining Attacks in Sharded Blockchains

Sheng-Wei Wang
Department of Electronic Engineering
National United University
Miaoli 360302, TAIWAN
swwang@nuu.edu.tw

***Abstract*—Sharding is a promising technology to improve scalability of a blockchain. A blockchain is partitioned into a number of shards each of which is maintained by a subset of miners. The multiple shards constitute a sharded blockchain and are able to process transactions concurrently such that the overall throughput is increased. However, decreasing the number of miners in a blockchain increases the possibility to be attacked. In this paper, we consider how selfish mining attacks sharded blockchains. To the best of our knowledge, the problem has not been studied before. We first formulate an optimization problem to maximize the rewards earned by selfish miners by using an accurate analytical model. An algorithm for selfish miners to earn most rewards is proposed. Numerical results show that robustness of blockchains becomes weak when the blockchain is sharded. However, no matter how many number shards in a sharded blockchain, the rewards earned by selfish miners are close to each other. Furthermore, when the honest mining rate is uniformly assigned to each shard, the selfish miners earns the smallest amount of rewards.**

***Index Terms*—Blockchain, selfish mining, sharding**

I. Introduction

Blockchain is a decentralized ledger which is originally used in Bitcoin network [1]. In a blockchain, transactions are securely stored in the blocks and the blocks are concatenated using cryptography. Besides the Bitcon transactions, blockchains are widely used in processing various aspects of data nowadays. For example, Ethereum provides blockchain platforms for developing smart contracts which process a large number of various transactions such as financial, health or sports records [2].

Main problem of blockchain technology is its scalability [3]. While Visa is able to process up to 24,000 transactions per second, Bitcoin and Ethereum can only process 7 and up to 30 transactions per second [4]. It is obvious that current blockchain is not appropriate for the applications with large number of transactions. A number of approaches such as sharding [5], Directed Acyclic Graph (DAG) [6] and Lightning Network [7], have been proposed to solve the scalability issues in blockchains [3].

Among the approaches, sharding is a promising technology to improve the scalability of a blockchain [5]. Main idea of sharding is to partition the nodes (miners) into a number of disjoint subsets. Miners in each subset maintain a sub-blockchain, namely, a *shard*, in which the transactions are also partitioned. Using sharding technology, the multiple shards are able to process transactions concurrently such that the throughput of the overall blockchain can be improved. In this paper, the multiple shards is said to constitute a sharded blockchain. We also called a sharded blockchain a K*-shard blockchain* if the number of shards equals to K.

Despite the advantages of sharding technology, some problems arise when the blockchain is sharded. The first problem is the large cross-shard communication overheads. In [8], there are at least 80% cross-shard transactions in a sharded blockchain. A cross-shard transaction shall be verified in multiple shards resulting in large communication overheads.

Another problem is the security issue [3]. The robustness of a blockchain depends on the number of nodes maintaining the blockchain. In a public blockchain, if malicious nodes are more than normal nodes, the blockchain will be dominated by the malicious nodes. This is called *51% attacks* [1]. When a blockchain is sharded, the nodes are partitioned into multiple subsets each of which is assigned to maintain a shard. Therefore, the number of nodes maintaining a shard decreased such that the robustness of the shards becomes weak.

Most of previous researches considered the malicious nodes which attack the consensus mechanism in sharded blockchains [9]–[13]. In this paper, we consider another type of attacks called *selfish mining attacks* [14] in sharded blockchains. The goal of selfish mining attacks is not to attack the consensus mechanism in a shard. Rather, the goal is to earn more rewards in an unfair manner. To the best of our knowledge, selfish mining attacks in sharded blockchains have not been studied before.

Main idea of selfish mining attack is to hide the mined block without notifying other miners. Such miners are called *selfish miners* and others are called *honest miners* otherwise. Since other miners are not notified that a block has been mined, they still spent their computation efforts in mining the mined block. Therefore, the computation efforts of other miners are wasted. In [14], the authors show that when the fraction of selfish mining rate is larger than 25%, the miner is *profitable*; that is, he can earn more than he is entitled to. On the other hand, if the fraction of a selfish miner's mining rate is less than 25%, he earns less than his entitled shares. The threshold that a selfish miner is profitable is called the *profitable threshold*. In a single blockchain with one selfish miner, the profitable threshold is 25%.

Selfish mining attack becomes much easier in sharded blockchains. Since the number of nodes are partitioned into different shards, the total mining rate in each shard is much smaller than that in the single blockchain. If the selfish miners

979-8-3503-7099-7/24/$31.00 ©2024 IEEE

intelligently assign their selfish mining rates to the shards, it is possible for them to lower the profitable threshold to less than 25%. In this paper, we investigate the impact of earned rewards when selfish mining attacks the sharded blockchains. We are interested in how sharding affects the rewards earned by selfish miners. Furthermore, we hope to study the relationships between the the number of shards and the rewards earned by selfish miners. We also considered how to defend the selfish mining attacks by carefully assigning honest mining rates into each shard.

An optimization problem is formulated to maximize earned rewards in a sharded blockchain. We then proposed an algorithm which optimally assigns the selfish mining rates to each shard such that the earned rewards are maximized. Numerical results show that robustness of the blockchain becomes weak when the blockchain is sharded. However, no matter how many shards are in a sharded blockchain, the rewards earned by selfish miners are close to each other. Finally, we found that the smallest reward earned by selfish miners occurs when the honest mining rates are uniformly assigned to each shard.

The rest of this paper is organized as follows. Selfish mining strategy is introduced in the next Section. The problem of maximizing earned rewards in sharded blockchains are formulated in Section III. An algorithm to solve the optimization problem is proposed and the earned rewards by using the proposed algorithm are derived in Section IV. Numerical results are then discussed. Finally, some concluding remarks are given.

II. Selfish Mining Attacks

Selfish mining attacks are first proposed in [14]. In the blockchain with one selfish miner, the selfish mining attacks operate as follows.

1) When the honest miner mined the block first and the selfish miner has no blocks in his private chain, the selfish miner acts as an honest miner to validate the block and to mine the next bock. In this situation, the honest miner earns 1 unit of reward.
2) When the selfish miner mined the block first, he keeps the block in a private chain and start to mine the next block after the mined block.
3) When the honest miner mined a block and there is one block in the selfish miner's private chain, the selfish miner publishes the block to create a competitive situation among the two branches. According to the *longest chain rule*, the first chain where the next block is mined will be considered as the valid chain [1]. In the competitive situation, the selfish miner may only mine the next block after the block on his private chain while the honest miner may mine the two chains simultaneously with half of his mining rate.
    - When the selfish miner mined the next block, it means that the selfish miner earns 2 units of rewards.
    - When the honest miner mined the next block after the block the selfish miner mined, the selfish miner and the honest miner both earn 1 unit of reward.
    - When the honest miner mined the next block after the block he mined, the honest miner earns 2 units of rewards.
4) When the honest miner mined the block and there are two private blocks on the selfish miner's chain, the selfish miner publishes the two blocks and becomes the public chain because the chain is the longest one. In this situation, the selfish miner earns 2 units of rewards.
5) When the honest miner mined the block and there is more than two private blocks owned by selfish miner, he will still keep his blocks in private until the difference between the private chain and public chain equals to 2. When the situation occurs, the selfish miner publishes all his private blocks and earns the rewards according to the length of his published chain.

In [14], the authors show that the selfish is profitable when the fraction of selfish mining rate is larger than 25%. The selfish mining strategy is criticized since the required selfish mining rate is too large such that it is impossible to form a mining pool with larger than 25% selfish mining rate in the Bitcoin network [15]. However, when the blockchain is sharded, the honest mining rate is distributed to different shards. It is possible for the selfish miners to have more than 25% mining rate and to affect the earned rewards significantly.

III. Problem Formulation

In this section, we calculate the rewards earned by the selfish miners in a sharded blockchain. We first introduce the notations used in this paper. The objective function is then derived. Finally, we formulate the optimization problem of maximizing the fractions of rewards earned by selfish miners.

A. Notations and definitions

In a blockchain, let h and s denote the total honest and total selfish mining rates respectively. Without loss of generality, we assume sum of the two mining rates equals to 1. That is,

$$h + s = 1 \tag{1}$$

The number of shards is denoted as K where the shards are labeled from shard 1 to shard K. Let h_i and s_i represent the honest and selfish mining rates in shard i where $1 \leq i \leq K$. Therefore, we have

$$\sum_{i=1}^{K} h_i = h \quad \text{and} \quad \sum_{i=1}^{K} s_i = s \tag{2}$$

.

Next, we calculate the fraction of earned rewards by selfish miners. Let $RW(\alpha)$ denote the fraction of rewards earned by a selfish miner with fraction of selfish mining rate α. A closed-form expression to calculate the value of $RW(\alpha)$ has been derived as follows [14].

$$RW(\alpha) = \begin{cases} 1 & \text{if } \alpha \geq 0.5, \\ \frac{\alpha(1-\alpha)^2[4\alpha+\frac{1}{2}(1-2\alpha)]-\alpha^3}{1-\alpha[1+(2-\alpha)\alpha]} & \text{otherwise} . \end{cases} \tag{3}$$

The function $RW(\alpha)$ is a convex function between 0 and 0.5.

Let R_i denote the earned rewards by selfish miners in shard i. That is,

$$R_i = RW(\frac{s_i}{h_i + s_i}) \tag{4}$$

The overall fraction of earned rewards earned by selfish miners in the sharded blockchain with K shards is as follows.

$$R = \frac{1}{K}\sum_{i=1}^{K} R_i = \frac{1}{K}\sum_{i=1}^{K} RW(\frac{s_i}{h_i + s_i}) \tag{5}$$

When the number of shards equals to 1, this is a blockchain without sharding technology and the rewards earned by selfish miners equals to $RW(s)$.

B. The optimization problem

From equation (3), we found that if mining rate of a selfish miner equals or larger than 50%, the selfish miner is said to *dominate* the blockchain and get all rewards from the blockchain. In sharded blockchains, selfish miners can optimally assign their mining rates to each shard such that overall fraction of rewards earned by selfish miners is maximized. Given the number of shards K, the honest mining rates h_i for all shards i, we formulate the optimization as follows.

$$\textbf{Maximize} \quad R = \frac{1}{K}\sum_{i=1}^{K} R_i \tag{6}$$

$$\textbf{With respect to} \quad s_i \ , \ \ \forall\ i = 1, 2, \cdots, K \tag{7}$$

Subject to constraints

$$\sum_{i=1}^{K} s_i = s \tag{8}$$

$$0 \le s_i \le s, \quad i = 1, \cdots, K \tag{9}$$

Since the objective function is a convex function, the optimization problem can be solved by one of the optimization techniques introduced in [16].

IV. The proposed algorithm

In this section, we proposed an algorithm to solve the optimization problem more efficiently. The rewards obtained by the algorithm are also analyzed and discussed.

A. The proposed algorithm

By observing the reward function shown in equation (3), we found that $RW(\alpha)$ is a strictly increasing function with respect to selfish mining rate α when $0 \le \alpha \le 0.5$. Furthermore, $RW(\alpha)$ is also a convex function. That is, when the value of α increases, $RW(\alpha)$ increases exponentially. Therefore, main idea of the proposed algorithm is to maximize the number of shards which are dominated by selfish miners. Based on the idea, we describe details of the proposed algorithm as follows.

1) Sort the shards in ascending order according to the values of honest mining rate on the shard h_i. Let the honest mining rates $h_1 \le h_2 \cdots \le h_K$. Let $\bar{s}$ denote the remaining selfish mining rate which has not been assigned. Initially, the remaining selfish mining rate $\bar{s}$ is set to total selfish mining rate s.
2) We start from shard 1. If $\bar{s} \ge h_1$ in shard 1, then $s_1 = h_1$. Remaining selfish mining rate $\bar{s} = \bar{s} - s_1$.
3) The algorithm iteratively checks the relationship between remaining selfish mining rate and the honest mining rate in a shard. The iteration terminates until $\bar{s} < h_{m+1}$ where shards 1 to m are dominated by selfish miners.
4) If the remaining selfish mining rate is larger than 0, the remaining selfish mining rate is all assigned to shard $m + 1$. Otherwise, the $s_{m+1} = 0$.
5) Finally, there will be no selfish miners mining in shards $m + 2$ to K.

B. Rewards analysis

We then analyzed the rewards earned by selfish miners using the proposed algorithm. Note that m represents the number of shards dominated by selfish miners. Therefore, the fractions of rewards in shards 1 to m earned by selfish miners all equal to 1.

Next, we calculated the rewards earned in shard $m + 1$. The remaining selfish mining rate s_{m+1} can be calculated as follows.

$$s_{m+1} = s - \sum_{i=1}^{m} s_i \tag{10}$$

The rewards of selfish miners on shard $m+1$ can be calculated by equation (3) where the fraction of selfish mining rate is $s_{m+1}/(h_{m+1} + s_{m+1})$.

In other shards, there is no selfish miners in the shards. They earn no rewards from the shards. Finally, the fraction of rewards earned by selfish miners R in the sharded blockchain is the average of fractions over all shards. That is,

$$\begin{aligned} R_s &= \tfrac{1}{K} \times [m \times 1 + 1 \times RW(\tfrac{s_{m+1}}{h_{m+1}+s_{m+1}}) \\ &\quad +0 \times (K - m - 1)] \\ &= \tfrac{1}{K} \times [m + RW(\tfrac{s_{m+1}}{h_{m+1}+s_{m+1}})]. \end{aligned} \tag{11}$$

We also consider a special situation that the honest mining rates are uniformly distributed into K shards; that is, the honest mining rate in each shard equals to $\frac{h}{K}$. In this situation, the number of shards m dominated by selfish miners can be calculated as follows.

$$m = \left\lfloor \frac{s}{\frac{h}{K}} \right\rfloor \tag{12}$$

The selfish mining rate s_{m+1} on shard $m + 1$ can be obtained by following equation.

$$s_{m+1} = s - m \times \frac{h}{K} \tag{13}$$

The fraction of rewards earned by selfish miners is derived in the following.

$$R_s = \frac{[m + RW(\frac{s_{m+1}}{h_{m+1}+s_{m+1}})]}{K} \tag{14}$$

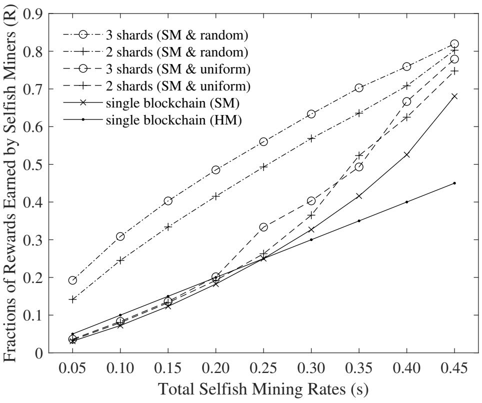

Fig. 1: Fractions of rewards earned by selfish miners with different number of shards and different honest miner distributions

V. Numerical results and discussions

Numerical results are studied to investigate the relationships between total selfish mining rates s and the rewards earned by selfish miners R in sharded blockchains . We compare the earned rewards in sharded blockchains with different number of shards too. Using the proposed algorithm, the rewards earned by selfish miners when honest miners are uniformly or randomly assigned to each shard are also studied.

In the following figures, honest and selfish mining strategies are labeled as *HM* and *SM* respectively. The strategy that honest mining rates are uniformly and randomly assigned each shard are labeled as *uniform* and *random* respectively. The maximum, minimum, and average fractions of rewards are respectively labeled as *max*, *min*, and *avg*. The data points which represent the randomly assigned honest mining rates are the average of 10^6 randomly combinations of mining rate assignments.

The number of shards in a sharded blockchain discussed in this paper is 2 and 3. When the number of shards is larger than 3, the sharded blockchains have similar properties as 2-shard or 3-shard blockchains. Therefore, we show the numerical results of 2-shard and 3-shard blockchains in this paper only.

We first compare the fractions of rewards earned by selfish miners with different number of shards and different distributions of honest mining rates. Fig. 1 shows the fractions of rewards earned by selfish miners with respect to different value of total selfish mining rates s. From the figure, we can make the following observations:

- Selfish mining strategy in a sharded blockchain enables selfish miners to earn more rewards than those in a single blockchain without sharding.
- When the honest mining rate is uniformly assigned to each shard in a sharded blockchain, the profitable threshold becomes to 21% which is lower than 25% in a single blockchain without sharding.
- When the honest mining rate is randomly assigned, the average fractions of rewards earned by selfish miners are always larger than the rewards earned by selfish mining strategies in a single blockchain or 2-shard blockchains.
- If the honest mining rate is randomly assigned, the rewards earned by selfish mining in a 3-shard blockchain is significantly larger than that in a 2-shard blockchain. However, if the honest mining rate is uniformly assigned, the earned rewards in 2-shard and 3-shard blockchains close to each other.

TABLE I: Rewards earned in 2-shard blockchain

$s = 0.34$, $h = 0.66$	h_i	s_i	R_i
Shard 1	0.33	0.33	1.0000
Shard 2	0.33	0.01	0.1680
Overall Rewards	0.5084		

TABLE II: Rewards earned in 3-shard blockchain

$s = 0.34$, $h = 0.66$	h_i	s_i	R_i
Shard 1	0.22	0.22	1.0000
Shard 2	0.22	0.12	0.4218
Shard 3	0.220	0	0
Overall Rewards	0.4739		

To explain why the earned rewards in 2-shard and 3-shard blockchains close to each other when the honest mining rate is uniformly assigned, we take $s = 0.34$ and $h = 0.66$ for example. Table I shows the assignment of selfish mining rates in 2-shard blockchain by using the proposed algorithm. Since the honest mining rate is uniformly assigned, the honest mining rate on each shard is 0.33. According to the proposed algorithm, selfish miner assigns 0.33 mining rates to shard 1 and 0.01 to shard 2. The fractions of rewards earned by selfish miners in shard 1 and 2 are 1 and $RW(0.01/(0.01 + 0.33))$ respectively. Finally, the fraction of rewards earned by selfish miners is $\frac{1}{2} \times 1 + \frac{1}{2} \times RW(0.01/0.34)$ which equals to 0.5084.

Table II shows the assignment of selfish mining rates. In 2-shard blockchain, the fraction of rewards earned by selfish miners is obtained as 0.4739. We observed that rewards earned in a 3-shard blockchain is less than those in a 2-shard blockchain. In both cases, we found that the selfish miner is able to earn all rewards in shard 1 and earn some rewards in shard 2. In 3-shard blockchain, the selfish miners assign no mining rate on shard 3 such that no rewards can be earned. In shard 1, selfish mining strategy earned 1/2 and 1/3 overall fractions of rewards earned by selfish miners in 2-shard and 3-shard blockchains respectively. In shard 2, selfish mining yield $0.1680/2$ and $0.4218/3$ overall fraction earned rewards in 2-shard and 3-shard blockchains respectively. Since the number of shards increases, the value of the rewards earned in each shard decreases. By considering the number of shards and fraction of earned rewards, we found that rewards earned in a 3-shard blockchain is less than those in a 2-shard blockchain. This observation shows that the number of shards is not the key parameter to affect the earned rewards earned by selfish miners.

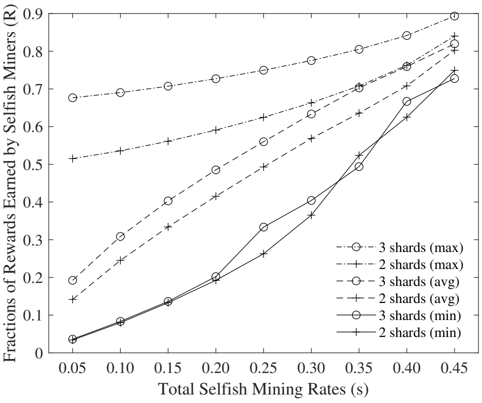

Fig. 2: Fractions of rewards earned by selfish miners when the honest mining rates are randomly assigned

Next, we discuss how sharded blockchains defends the selfish mining attacks. The idea is to carefully assign honest mining rate to each shard. Given an honest mining rate h, we randomly select the mining rates on each shard as the value of h_i on shard i. The sum of h_i over all shard i shall equal to h. The proposed algorithm is applied to assign the selfish mining rate on each side from the shard with smallest honest mining rate. The algorithm repeats 10^6 times. The maximum, minimum, and average fractions of rewards earned by selfish miners are recorded.

Fig. 2 shows the maximum, minimum, and average fractions of earned rewards when the number of shards equals to 2 and 3 when the honest mining rate is randomly assigned. From the figure, we can make the following observations.

- The maximum and average fractions of rewards in 3-shard blockchains are always larger than those in 2-blockchain. The minimum fractions of rewards in 2-shard and 3-shard blockchains close to each other.
- The maximum fractions of earned rewards occur when the honest mining rates on shard 1 (2-shard blockchain) or those on shard 1 and 2 (3-shard blockchain) are both very small. The minimum fractions occur when the honest mining rate is uniformly assigned. Therefore, we can conclude that if a sharded blockchain hopes to lower the rewards earned by selfish miners, the best strategy is to uniformly assign the honest mining rates to each shard.

VI. Conclusions and Future Works

In this paper, we consider the selfish mining attacks in sharded blockchains. Sharding technology improves the scalability of a blockchain while some security issues arise. Since the honest mining rate are distributed to a number of shards, honest mining rate in each shard decreases significantly. In such situation, selfish mining is able to get advantage in sharded blockchains by optimally assigning the selfish mining rate to each shard due to small honest mining rate.

We formulate an optimization problem to study the maximum fraction of rewards can be earned by selfish miners. An algorithm is proposed and the earned rewards are then analyzed. Some interesting conclusions can be made by observations on the numerical results:

- Selfish miners are able to earn more rewards in a sharded blockchain than in a single blockchain without sharding.
- The number of shards in a sharded blockchain does not affect the earned rewards significantly.
- If the honest mining rate is not uniformly assigned to each shard, selfish mining is able to earn more rewards. Therefore, the honest miners earns less rewards than those in a single blockchain without sharding. In order to keep the security of a sharded blockchain, the honest mining rate shall be assigned to each shard randomly.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized business review*, p. 21260, 2008.

[2] G. Wood *et al.*, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, no. 2014, pp. 1–32, 2014.

[3] A. Hafid, A. S. Hafid, and M. Samih, "Scaling blockchains: A comprehensive survey," *IEEE Access*, vol. 8, pp. 125 244–125 262, 2020.

[4] M. Conti, E. Sandeep Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3416–3452, 2018.

[5] G. Wang, Z. J. Shi, M. Nixon, and S. Han, "Sok: Sharding on blockchain," in *Proceedings of the 1st ACM Conference on Advances in Financial Technologies*, ser. AFT '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 41–61. [Online]. Available: https://doi.org/10.1145/3318041.3355457

[6] H. Pervez, M. Muneeb, M. U. Irfan, and I. U. Haq, "A comparative analysis of dag-based blockchain architectures," in *2018 12th International Conference on Open Source Systems and Technologies (ICOSST)*, 2018, pp. 27–34.

[7] J. Poon and T. Dryja, "The bitcoin lightning network: Scalable off-chain instant payments," 2016.

[8] C. Li, H. Huang, Y. Zhao, X. Peng, R. Yang, Z. Zheng, and S. Guo, "Achieving scalability and load balance across blockchain shards for state sharding," in *2022 41st International Symposium on Reliable Distributed Systems (SRDS)*, 2022, pp. 284–294.

[9] X. Huang, Y. Wang, Q. Chen, and J. Zhang, "Security analyze with malicious nodes in sharding blockchain based fog computing networks," in *2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall)*, 2021, pp. 1–5.

[10] X. Chen, "Scaling byzantine fault-tolerant consensus with optimized shading scheme," *IEEE Transactions on Industrial Informatics*, pp. 1–12, 2023.

[11] A. Kumar, A. Sangoi, S. Raj, and K. M, "Shardcons - a sharding based consensus algorithm for blockchain," in *2021 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*, 2021, pp. 1–6.

[12] D. Yu, H. Xu, L. Zhang, B. Cao, and M. A. Imran, "Security analysis of sharding in the blockchain system," in *2021 IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 2021, pp. 1030–1035.

[13] Y. Liu, X. Xing, H. Cheng, D. Li, Z. Guan, J. Liu, and Q. Wu, "A flexible sharding blockchain protocol based on cross-shard byzantine fault tolerance," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 2276–2291, 2023.

[14] 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.

[15] D. C. S. Wright and S. Savanah, "The fallacy of the selfish miner in bitcoin: An economic critique," *Available at SSRN 3009466*, 2017.

[16] W. Sun and Y.-X. Yuan, *Optimization theory and methods: nonlinear programming*. Springer Science & Business Media, 2006, vol. 1.