Committee Selection Based on Game Theory in Sharding Blockchain

Jingrou Wu and Jin Zhang(✉)

Southern University of Science and Technology, Shenzhen 518055, China
11960005@mail.sustech.edu.cn, zhangj4@sustech.edu.cn

Abstract. Blockchain has attracted the public's attention in recent years as a decentralized system. But it suffers from low transaction throughput and poor scalability. Sharding technology is proposed to improve blockchain's efficiency and performance using parallel processing. The key idea is to divide the miners into different shards or committees to process disjoint transaction sets. There are two kinds of committees in the sharding blockchain which bring miners different costs and rewards. One is dedicated to membership management and cross-shard transaction routing while the other is responsible for transaction validation. Miners have to decide which committee to participate in before they start working. In this paper, we study the problem of how much computational power would miners contribute to different kinds of committees in the view of game theory. We model the game as a two-stage hierarchical game and obtain the Nash equilibrium of this game. The experimental results show that both computational power limitation and system's parameters have effects on the final equilibrium.

Keywords: Proof of work · Sharding blockchain · Game theory

1 Introduction

The past decade has witnessed the rapid development of the blockchain since Satoshi Nakamoto proposed *Bitcoin* cryptocurrency in 2008 [17]. A blockchain is a transparent and traceable decentralized database with most miners' consensus. In a permissionless blockchain such as Bitcoin and Ethereum [23], proof of work (PoW) is the most common consensus protocol which requires computational power to solve PoW hash puzzles. High cost of PoW puzzles prevents malicious miners from attacking the blockchain system but it also leads to low transaction throughput and poor scalability.

To solve the efficiency problem, researches are conducted in scalability and throughput improvement, among which *sharding protocol* is a more general solution in blockchains' performance enhancement. Sharded blockchains allow miners to process diverse sets of transactions at the same time. Miners are divided into several shards or committees in which miners gather and process different sets of transactions in different shards. The shard size is unalterable because a larger

K. Wu et al. (Eds.): ICECI 2021, LNICST 437, pp. 13–28, 2022.
https://doi.org/10.1007/978-3-031-04231-7_2

shard size lowers the efficiency while a smaller shard size heightens the risk. The number of shards also keeps fixed as the network size is stable.

Miners' identities and group information need recording in the sharded blockchain system. In a permissioned system such as RSCoin [7], a trusted third-party, i.e., the central bank, is responsible for record and registration. While in a permissionless system without any trusted third-party such as RapidChain [25], a special committee, *Directory Service (DS) committee* or *Reference committee*, is required instead. Miners firstly compete for joining the DS committee. Then the rest miners compete for other shards' members. Since different kinds of committees bring different rewards and costs, it becomes a question for miners to decide which kind of committee to participate in and how much computational power to put in.

In non-sharding blockchain systems, especially Bitcoin, there are many studies to analyze miners' optimal actions. Most works [3,8,22] focus on participation of miners. That is, whether they join or leave in a non-sharding PoW blockchain. The computational power allocation is another field where miners decide how much computational power for investment [5,9]. However, these game models are not suitable in sharded blockchains because of different decision spaces and reward protocols. In the work [16], it analyzes actions of miners in a sharded blockchain with only non-DS committees hence they have no committee selection problem.

In this paper, we investigate the problem of miners decisions on different kinds of committees. We model the process as a two-stage hierarchical non-cooperative game. In the first stage, miners compete for the seat of the DS committee and then those who are not DS committees members play games during shards formation in order to maximize their utilities. The main contributions are as follows.

- We model the committee selection problem as a two-stage hierarchical game among miners.
- We prove the existence of Nash equilibrium of both sub-games. Further, we prove the uniqueness of Nash equilibrium of the DS committee member selection sub-game, i.e., the stage 1 sub-game.
- We conduct simulations to find that the game converges to the Nash equilibrium in practice and the experimental results show that computational power limitations affect miners' final decisions.

The rest of the paper is organized as follows. Section 2 describes the details of sharding protocols and Sect. 3 formulates the two-stage game model followed by Sect. 4 which gives an analysis of the Nash equilibrium in both sub-games. The experimental results are shown in Sect. 5 and related work are included in Sect. 6. We present the conclusion of the paper in Sect. 7.

2 Sharding Fundamentals

In this section, we firstly present the concept of sharded blockchain in detail and then describe the process of a blockchain with shards.

To support higher scalability and efficiency, the sharded blockchain partitions miners into different groups called shards or committees. Every shard can be regarded as a sub-network of the blockchain. Miners in the same shard process the same set of transactions by running Byzantine Fault-Tolerant (BFT) protocols (e.g. PBFT [4]) rather than PoW consensus protocols due to the small size of the shard. Therefore, the sharded blockchain is able to deal with different sets of transactions in parallel. The miners are chosen by PoW hash puzzles to join in these shards, which prevents Sybil Attack and guarantees miners' abilities to an extent. Given a sharded blockchain with a stable number of miners, the size of the shard and the number of shards remains fixed to keep a balance between efficiency and security. If there are more miners than required, some of them are not able to become shard members.

Meanwhile, a special committee, DS committee or reference committee, is required in the system for shards information record and miners registration. It is also responsible for cross-shard transactions which are transactions related to more than one shard. The DS committee provides routing services for such transactions. Besides, it aggregates micro blocks produced by other shards into the final block in the blockchain. Based on these functions, the DS committee members must be selected at first before other shards members. There are several diverse *DS committee member election* methods, among which the PoW puzzle is a common choice such as in Zilliqa [1]. To maintain the fixed size of the DS committee, the first-in-first-out policy is applied. The earliest committee member quits the DS committee and then the miner who solves the PoW puzzle at first becomes the new member. Overall, the DS committee and other shards have different duties in the sharded blockchain system and have different PoW puzzles to solve during selection.

For the sake of fairness, all committees shuffle after a period of time called *epoch* in order to prevent collusion. At the beginning of the epoch, the DS committee is formed firstly and then other shards are shaped. After committee formations, miners process transactions in parallel, generating m micro blocks for each shard during the epoch. At the end of the epoch, the system distributes rewards to miners and miners prepare themselves for the next epoch.

3 Committee Selection Game

In this section, we formulate the committee selection game as a two-stage hierarchical game. We assume all miners are honest but selfish and miners do not collude with each other. To maximize their own utilities, miners decided the amount of computational power to contribute to different committee formation processes.

3.1 Problem Formulation

We consider the situation where miners are able to make decisions to contribute how much computational power to the first PoW hash puzzle PoW_1 and the

second puzzle PoW_2 on themselves. They are selfish and therefore they only care about their own profits while doing choices. We formulate the Computational Power Game $\mathbb{G}$ as a non-cooperative game denoted by $\mathbb{G} = (\mathcal{P}, \mathcal{S}, \mathcal{U})$, where $\mathcal{P}$ is a set of players, $\mathcal{S}$ is the players' strategy space and $\mathcal{U}$ is the players' utility values.

Players ($\mathcal{P}$). Players are miners who are willing to participate in the game including *DS Committee Member Selection* as well as *Shards Formation*, at a given epoch. The DS committee with the size of n_1 requires 1 new member and other shards need n_2 miners at a time. Let's assume all players are shortsighted which means they only aim at the current game without considering the following repeated game processes. At a one-shot game, they make decisions merely dependent on the final utility.

With N players of computational power limitations $\bar{\mathbf{X}} = \{\bar{x_1}, \bar{x_2}, \cdots, \bar{x_N}\}$ in a game, players firstly play the DS Committee Member Selection sub-game where only one player is able to become the new committee member. Then the rest $N-1$ players compete for n_2 seats in shards.

Strategies ($\mathcal{S}$). For each sub-game, the strategies of players are to decide the amount of computational power x_i to put in. If the computational power $x_i = 0$, it means that the player does not participate in the process.

In the stage 1 sub-game, miners contribute computational power to solve the PoW_1 puzzle. Once the ith miner has been chosen as a new member, he would sign $m+m_e$ signatures where m is the number of other shard members' signatures and m_e is the number of extra signatures as a DS committee member. Given the total system reward R, a part of reward aR is distributed to $N_s = n_1 + n_2$ all committee members as fixed reward $r_f = \frac{aR}{N_S}$, while the rest reward $(1-a)R$ is assigned to members according to their workload, i.e., the number of signatures. Every valid signature is rewarded with $r_s = \frac{(1-a)R}{N_s m + n_1 m_e}$. Hence, the reward of a DS committee member is composed of two parts, the fixed reward r_f and the workload reward $r_s(m + m_e)$:

$$r_1 = r_f + r_s(m + m_e) \tag{1}$$

Similarly, in the stage 2 sub-game, successful miners with m signatures gain r_2 with a fixed component r_f and a workload component $r_s m$ as follows:

$$r_2 = r_f + r_s m \tag{2}$$

Utilities ($\mathcal{U}$). Given the rewards mentioned above, we consider the expectation of rewards as profits for every miner.

$$r_{1,i} = p(x_i; \mathbf{X_{-i}}) r_1 \tag{3}$$

$$r_{2,i} = p(x_i; \mathbf{X_{-i}}) r_2 \tag{4}$$

where $p(x_i; \mathbf{X_{-i}})$ is the probability of the ith miner becoming a committee member.

The cost is composed of 4 aspects: (1) the boot loss cost for PoW puzzle solving, (2) the energy cost, (3) the cost for signatures and (4) the cost for fixed assets depreciation, which is denoted by:

$$c(x_i, m_i) = c_f x_i + c_e t x_i + c_s m_i + c_r \frac{x_i}{\bar{x_i}} \tag{5}$$

where $c_f x_i$ is the boot loss cost for using x_i computational power, $c_e t x_i$ is the energy cost with t the time for solving the PoW puzzle, $c_s m_i$ is the workload cost and $c_r \frac{x_i}{\bar{x_i}}$ is the fixed assets depreciation cost.

We assume that are enough miners in every epoch to form committees. In this way, the miner's utility is equal to the expectation of the rewards minus the cost:

$$U(x_i; \mathbf{X_{-i}}) = p(x_i; \mathbf{X_{-i}})r - c(x_i, m_i) \tag{6}$$

where $\mathbf{X_{-i}} = \{x_1, x_2, \ldots\}$ is a vector of other miners' strategies, r is the general symbol of reward and m_i is the number of signatures the ith miner will sign. The details of utility are analyzed in Sect. 3.2.

3.2 Hierarchical Game Model

Because the DS committee member selection and shards formation are two different processes, we model the game $\mathcal{G}$ as a two-stage game, the stage 1 DS committee member selection game (CSG) and the stage 2 shards formation game (SFG) $\mathcal{G}_2$. All miners firstly participate in $\mathcal{G}_1$ and then miners who fail to become a DS committee member compete for $\mathcal{G}_2$.

DS Committee Member Selection Sub-game. In this sub-game, only one player is able to get into the new DS committee which is similar to Bitcoin where only one block is generated in a period of time. We consider the PoW puzzles solving as a random process in which miners have to try a certain of times to find the final solution. It is formulated as *Poisson process* in former works [19,21,22]. We assume that unit computational power is able to find s possible answers per unit time and it requires k_1 attempts on average to solve the PoW_1 puzzle. We define the difficulty factor as $d_1 = \frac{k_1}{s}$ and hence the time required for finding one puzzle solution is drawn from the exponential distribution with a parameter $\theta = \frac{d_1}{x_i + Y}$ where $Y = \sum_{i \neq j} x_j$ is the total computation power in the system except for x_i. That is, the expectation of the time for the first solution found is θ. It is also the time t required for any players in this sub-game because whenever a solution is found, all other miners stop solving. As for the probability, it is only related to the computational power due to the memoryless property of the exponential distribution. It is represented as $p(x_i; \mathbf{X_{-i}}) = \frac{x_i}{x_i + \sum_{j \neq i} x_j}$. Therefore, the utility for players in this sub-game is the reward minus cost:

$$U_1(x_i; \mathbf{X_{-i}}) = \frac{x_i}{x_i + \sum_{j \neq i} x_j} r_1 - c(x_i, m + m_e) \tag{7}$$

where r_1 is the reward of the DS committee member and $c(x_i, m+m_e) = c_f x_i + c_e d_1 \frac{x_i}{x_i+Y} + c_s(m+m_e) + c_r \frac{x_i}{\bar{x}_i}$ is the cost.

We define the best response problem of stage 1 sub-game as:

Definition 1. *The best response problem of the DS committee selection sub-game (PoW_1) can be formulated as:*

$$\max_{0 \le x_i \le \bar{x}_i} U_1(x_i; \mathbf{X_{-i}}) \tag{8}$$

which means to find the best strategy, i.e., the amount of computational power to maximize the miner's utility.

Shards Formation Sub-game. In this sub-game, n_2 out of $N-1$ players are chosen as shard members. Different from the DS committee selection sub-game in Sect. 3.2, time for solving PoW_2 puzzles is not able to be drawn from total computational power because once a player successfully finds the solution, the process becomes a different Poisson process. Since it is difficult to predict which player has been selected as a new member, it is unpractical to model the time t from the view of total computational power. We formulate the time t in the aspect of individual solving process. That is, for each player, the process of PoW puzzle solving is a Poisson process with the parameter $\theta = \frac{d_2}{x_i}$ where $d_2 = \frac{k_2}{s}$ is the PoW_2's difficulty coefficient and k_2 is the number of attempts to find a solution. We assume that the DS committee publishes shards information after the window size t_2 and hence for those who are not selected as new members, they keep looking for a solution for t_2 as well. The probability of success is a sum of possibilities where the miner is chosen at jth:

$$p_2(x_i; \mathbf{X_{-i}}) = \sum_{j=1}^{n_2} p_{2,\mathbf{X_j}}(x_i; \mathbf{X_{-i}}) \tag{9}$$

where $\mathbf{X_j}$ is the set of permutations of miners' computational power when the ith miner's decision x_i at the jth position.

The probability of a miner with x_i computational power chosen as the jth shard member is the sum of probability for every permutation in $\mathbf{X_j}$:

$$p_{2,\mathbf{X_j}}(x_i; \mathbf{X_{-i}}) = \sum_{\mathbf{x_j} \in \mathbf{X_j}} \prod_{k=1}^{n_2} \frac{x_{j_k}}{Y + x_i - \sum_{l=1}^{k-1} x_{j_l}} \tag{10}$$

where $\mathbf{x_j}$ is the element (permutation) of the set $\mathbf{X_j}$ and x_{j_k} means the computational power of the kth miner in the permutation $\mathbf{x_j}$.

For example, if there are 3 players compete for 2 seats, the probability $p_2(x_i; X_{-i}) = \frac{x_i}{Y+x_i} + \sum_{j \in N} \frac{x_j}{Y+x_i} \cdot \frac{x_i}{Y+x_i-x_j}$ after simplifications is the sum of the possibility for the first competition and the possibility for the second competition. Hence the utility for players in this sub-game is composed of the two parts: (1) When the miner succeeds, the utility is the rewards minus the cost

with $\frac{d_2}{x_i}$ time and (2) When the miner fails, the utility is the cost only with t_2 time. Since the miner has the probability of p_2 for success, the utility is simplified as:

$$U_2(x_i; \mathbf{X_{-i}}) = p_2(x_i; \mathbf{X_{-i}})R_2 - Cx_i \tag{11}$$

where $R_2 = r_2 + c_e t_2 x_i - c_e d_2 - c_s m$ and $C = c_e t_2 + c_f + \frac{c_r}{\bar{x}}$.

Similarly, we define the best response of stage 2 sub-game as:

Definition 2. *The best response of shards formation sub-game PoW_2 can be formulated as:*

$$\begin{aligned} &\max_{0 \le x_i \le \bar{x}_i} U_2(x_i; \mathbf{X_{-i}}) \\ &\text{s.t.} \quad x_{PoW_1} \notin \mathbf{X_{-i}} \end{aligned} \tag{12}$$

where x_{PoW_1} is the computational power of the miner who has become a DS committee member.

4 Game Analysis

In this section, we provide the analysis of the two-stage game $\mathcal{G}$. We show that it exists a unique Nash equilibrium [18] in this game $\mathcal{G}$, which defines the optimal strategy for miners in both stages.

We firstly prove the existence of Nash equilibrium in stage 1 sub-game which is further proved to be unique. Then, we give a solution of shards formation sub-game based on the stage 1's result. In the next round $t+1$, validators change their strategies according to the difference between the utility of online and the utility of offline given their own network conditions and the current states $D_i(\theta_i, A_{t+1})$ where A_{t+1} is all players' decisions at the round $t+1$.

4.1 DS Committee Member Selection Sub-game

We analyze players' decisions in DS committee selection game here. According to (8), the utility of a player does not only subject to his own computational power contributed but also depends on others' behaviours. Given others' choices $\mathbf{X_{-i}} = \{x_1, x_2, \ldots\}$, the *ith* miner chooses the proper computational power x_i to maximize his utility, namely, $x_i = \arg\max_{0 \le x_i \le \bar{x}_i} U_1(x_i; \mathbf{X_{-i}})$. In a non-cooperative game, the *ith* miner uses this x_i as his best response which is stated in the following theorem.

Theorem 1 (Best response). *Given $\mathbf{X_{-i}}$, the best response of ith miner in DS committee member selection sub-game is*

$$x_i^* = \begin{cases} \sqrt{\frac{AY}{c_i}} - Y, & \textit{otherwise} \quad (13a) \\ 0, & \sqrt{\frac{AY}{c_i}} < Y \quad (13b) \end{cases}$$

where $A = r_1 - c_e d_1$ and $c_i = c_f + \frac{c_r}{\bar{x}_i}$

Proof. We use $U_{1,i}$ to denote the the utility of the *ith* miner in the DS committee member selection sub-game. The first and second derivatives of $U_{1,i}$ respect to x_i are:

$$\frac{\partial U_{1,i}}{\partial x_i} = \frac{AY}{(x_i + Y)^2} - c_i \tag{14}$$

$$\frac{\partial^2 U_{1,i}}{\partial x_i^2} = -\frac{2AY}{(X + Y)^3} \tag{15}$$

The second derivative of $U_{1,i}$ with respect to x_i is always negative so that $U_{1,i}$ is a concave function in x_i. Let the first derivative of $U_{1,i}$ with respect to x_i become zero. Then, $x_i = \sqrt{\frac{AY}{c_i}} - Y$. If $\sqrt{\frac{AY}{c_i}} - Y < 0$, it means that no matter how much computational power the player contribute, it always brings negative utility. Therefore, the player will not participate in the stage 1 sub-game and hence $x_i = 0$.

Now we consider the situation under the Nash equilibrium in which every player has his own best response $x_i^*, i \in N$ and none of them will alter the strategy because they will not get more rewards in such case. We prove that such Nash equilibrium is unique.

Theorem 2 (Uniqueness of Nash equilibrium). *There exists a unique Nash equilibrium in DS committee member selection sub-game and the optimal computation power for each player is given by* (13a) *and* (13b).

Proof. It is proven in [24] that if the best function is positive, monotonic and scalable, the game has a unique Nash equilibrium. So we prove these properties of the best function as follows.

Under the Nash equilibrium, every player makes his best response with respect to others' strategies. So, the computational power should be:

$$x_i^* = \sqrt{\frac{AY^*}{c_i}} - Y^* \tag{16}$$

where $Y^* = \sum_{i \neq j} x_j^*$.

We add Y^* on both side and the square of it is $(x_i^* + Y^*)^2 = \frac{AY}{c_i}$ so we have

$$x_i^* = CP^* - \frac{CP^{*2} c_i}{A} \tag{17}$$

where $CP^* = \sum_{i \in \mathbf{X}} x_i^*$. Sum up all the N equations of each player, we get

$$CP^* = \frac{(N-1)A}{\sum_{i \in N} c_i} \tag{18}$$

Replace CP^* with (18), we can get

$$x_i^* = \frac{(N-1)A}{\sum_{i \in N} c_i} - \frac{(\frac{(N-1)A}{\sum_{i \in N} c_i})^2 c_i}{A} \tag{19}$$

It is easy to prove this is a positive, monotonic and scalable function. Hence, the sub-game has unique Nash equilibrium.

4.2 Shards Formation Sub-game

Since players in this stage have already known about who has been chosen as a new DS committee, they only play game with the rest $N-1$ players. Similarly, the miners' strategies are the set of computational powers $\mathbf{X} = \{x_i | 0 \leq x_i \leq \bar{x_i}\}$ and utility functions are analyzed above.

Theorem 3 (Existence of Nash equilibrium). *There exists at least one Nash equilibrium in shards formation sub-game (choosing n_2 from $N-1$ miners) when $\bar{Y} < \frac{(n_2+1)B}{2c_e t_2}$, where $B = r_2 - c_e d_2 - c_s m$, $\bar{Y} = \sum_{j \neq i} \bar{x_j}$ and $n_2 \geq 2$.*

Proof. According to [12], when the strategy set is compact and convex and the utility function is a continuous function in the profile of strategies $\mathbf{s} \in \mathcal{S}$ and quasi-concave in s_i for every player, the game has at least one pure-strategy Nash equilibrium. Since the strategy set is compact and convex and the utility function is continuous obviously, we only need to prove its quasi-concave.

Because concave functions are always quasi-concave, we prove the concavity of the utility function in the following.

Lemma 1 (Concave utility function). *The utility function $U_2(x_i; \mathbf{X_{-i}})$ of miners in $\mathcal{G}_2$ is concave when $\forall n_2 \geq 2, \bar{Y} < \frac{(n_2+1)B}{2c_e t_2}$.*

Proof. We present the utility function $U_2(x_i; \mathbf{X_{-i}})$ and the probability function $p_2(x_i; \mathbf{X_{-i}})$ of the *ith* miner as $U_{2,i}$ and $p_{2,i}$ respectively. The first derivative of the utility function is

$$\frac{\partial U_{2,i}}{\partial x_i} = \frac{\partial p_{2,i}}{\partial x_i} R_{2,i} + p_{2,i} \frac{\partial R_{2,i}}{\partial x_i} - C \tag{20}$$

and the second derivative is

$$\begin{aligned} \frac{\partial^2 U_{2,i}}{\partial x_i^2} = & \frac{\partial^2 p_{2,i}}{\partial x_i^2} R_{2,i} \\ & + 2 \frac{\partial p_{2,i}}{\partial x_i} \frac{\partial R_{2,i}}{\partial x_i} \\ & + \frac{\partial^2 R_{2,i}}{\partial x_i^2} p_{2,i} \end{aligned} \tag{21}$$

where $U_{2,i}$ and $p_{2,i}$ are the utility and probability function of the *ith* miner in stage 2 sub-game.

Because $R_{2,i}$ is the linear function and hence $\frac{\partial^2 R_{2,i}}{\partial x_i^2} = 0$. Therefore, we have $\frac{\partial^2 R_{2,i}}{\partial x_i^2} p_{2,i} = 0$. We only need to prove $\frac{\partial^2 p_{2,i}}{\partial x_i^2} R_{2,i} + 2 \frac{\partial p_{2,i}}{\partial x_i} \frac{\partial R_{2,i}}{\partial x_i} < 0$ subject to $\bar{Y} < \frac{n_2(N-1)B}{2(N-n_2)C_e t_2}$.

After simplification, the first derivative of the probability function $p_{2,i}$ of the *ith* miner is:

$$\frac{\partial p_{2,i}}{\partial x_i} = \sum_{\mathbf{x_j} \in \mathbf{X_j}} \sum_{k=1}^{j-1} \frac{\prod_{l=1}^{j-1} x_{jl}}{\prod_{s=0}^{j-2} (Y + x_i - \sum_{l=1}^{s} x_{jl})^{a_k(s)}} \tag{22}$$

where $j = n_2 + 1$ and $a_k(s)$ is:

$$a_k(s) = \begin{cases} 2, & s = k, \\ 1, & s \neq k. \end{cases} \tag{23}$$

The second derivative has similar structure, summing up all second derivative of items listed above. We present the second derivative of the kth single item $T_k = \frac{\prod_{l=1}^{j-1} x_{j_k}}{\prod_{s=0}^{j-2}(Y+x_i-\sum_{l=1}^{s} x_{j_l})^{a_k(s)}}$ for example.

$$\frac{\partial T_k}{\partial x_i} = \sum_{s=0}^{j-2} \frac{-(a_k(s)+1)}{(Y + x_i - \sum_{l=1}^{s} x_{j_l})} T_k \tag{24}$$

If we prove that $F_k = \frac{\partial T_k}{\partial x_i} R_{2,i} + 2T_k c_e t_2 < 0$ for every single item in the first derivative of $p_{2,i}$, then we have $\frac{\partial^2 p_{2,i}}{\partial x_i^2} R_{2,i} + 2\frac{\partial p_{2,i}}{\partial x_i}\frac{\partial R_{2,i}}{\partial x_i} < 0$.

We can transform the F_k as:

$$\begin{aligned} F_k &= c_e t_2 \left(\frac{\partial T_k}{\partial x_i}\left(\frac{B}{c_e t_2} + x_i\right) + 2T_k\right) \\ &= T_k c_e t_2 \left(\sum_{s=0}^{j-2}\left(D_s\left(\frac{B}{c_e t_2} + x_i\right) + \frac{2}{n_2}\right)\right) \end{aligned} \tag{25}$$

where $D_s = \frac{-(a_k(s)+1)}{(Y+x_i-\sum_{l=1}^{s} x_{j_l})}$.

We only need to prove $Q(x_i) = \sum_{s=0}^{j-2} D_s(\frac{B}{c_e t_2} + x_i) + \frac{2}{n_2}$ is less than 0 because $T_k c_e t_2$ is always positive. Since it is a monotonically decrease function respect to x_i, we just need prove $Q(0) < 0$ when $x_i = 0$.

$$\begin{aligned} Q(0) &= \sum_{s=0}^{j-2} \frac{-(a_k(s)+1)}{(Y - \sum_{l=1}^{s} x_{j_l})} \frac{B}{c_e t_2} + \frac{2}{n_2} \\ &< \sum_{s=0}^{j-2} \frac{-(a_k(s)+1)}{Y} \frac{B}{c_e t_2} + \frac{2}{n_2} \\ &= \frac{-(n_2+1)}{Y} \frac{B}{c_e t_2} + 2 \\ &< \frac{-(n_2+1)}{\bar{Y}} \frac{B}{c_e t_2} + 2 \end{aligned} \tag{26}$$

Let $\frac{-(n_2+1)}{\bar{Y}} \frac{B}{c_e t_2} + 2 < 0$, we have $\bar{Y} < \frac{n_2+1}{2} \frac{B}{c_e t_2}$ which is consistent with the condition.

Hence, $U_2(x_i; \mathbf{X_{-i}})$ is concave when $\bar{Y} < \frac{(n_2+1)B}{2c_e t_2}$.

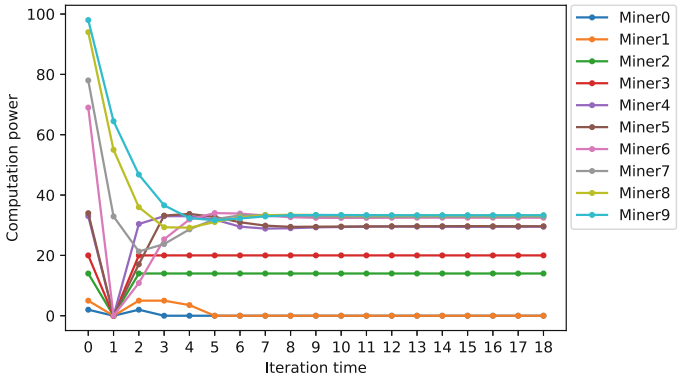

Fig. 1. Iterations in CSG.

5 Experimental Results

In this section, we conduct numerical simulations to find the Nash equilibrium in practical and evaluate different parameters' effects on players' strategies and utilities.

5.1 Game Analysis

The setting of our simulations are as follows. It has total $N = 10$ miners and $n_2 = 2$ required in other shards. The total reward is $R = 500$ and the reward ratio is $a = 0.75$. There are $m = 100$ blocks in an epoch. The cost coefficients are as follows: the electricity cost $c_e = 1$, the boot loss cost and the fixed assets depreciation cost $c_f = c_r = 0.5$ and the cost of each signature is ignored, that is, $c_s = 0$. The difficulty degrees are $d_1 = 2$ and $d_2 = 1$. The window size of the stage 2 process is $t_2 = 2$. In the one-short game, miners originally contribute the maximum computational power and their computational power limits are $\bar{\mathbf{X}} = \{2, 5, 14, 20, 33, 34, 69, 78, 94, 98\}$. As Fig. 1 and Fig. 2 shows, most players after several iterations converge to their final strategies where the $5th$ miner (Miner4) is chosen as the new DS committee member. Players with higher computational power are more likely to contribute more as well.

Figure 3 shows the final computational power miners contribute and the expectation of utilities they gain in both stages where the $5th$ miner (Miner4) is starred as a new DS committee member. Miners with less computational power are not willing to participate in the selection game while those who have more computational power are not likely to put all into the game. Compared the stage 1 with the stage 2, we found that players with high computational power would like to contribute more to stage 2 than stage 1 because they are more likely to be chosen in stage 2 than stage 1.

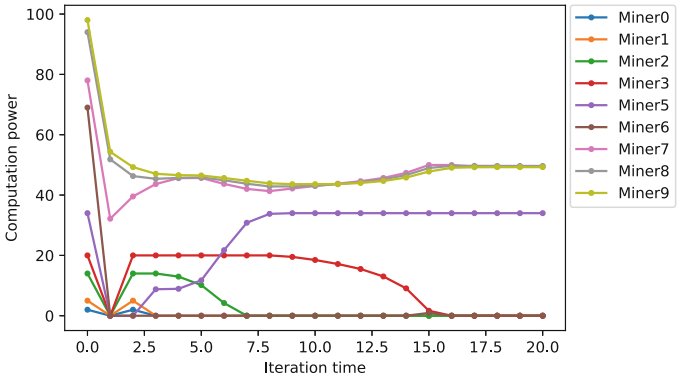

Fig. 2. Iterations in SFG.

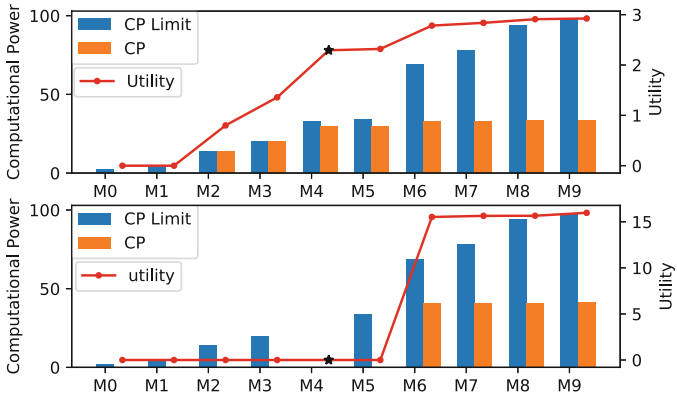

Fig. 3. Computational power and utility

5.2 Cost Coefficients Analysis

In this subsection, we draw attention to the impact of system parameters, especially the cost coefficients. All analyses are based on the stage 1 sub-game since stage 2 sub-game has a similar tendency.

In the setting as mentioned above, it presents that with the increase of the electricity cost c_e, miners are less likely to contribute computational power to the game. However, they receive more rewards because the computational powers of others decrease and therefore they have higher probabilities of success. In Fig. 4, we show some typical miners' computation powers and utilities where a miner gives up the game, a miner always put all computational power into the game and two other miners adjust their computational powers according to different electricity cost.

Different from the effect of electricity cost, the impacts of the boot loss c_f are more complex. When c_f is small, every player is willing to contribute all their

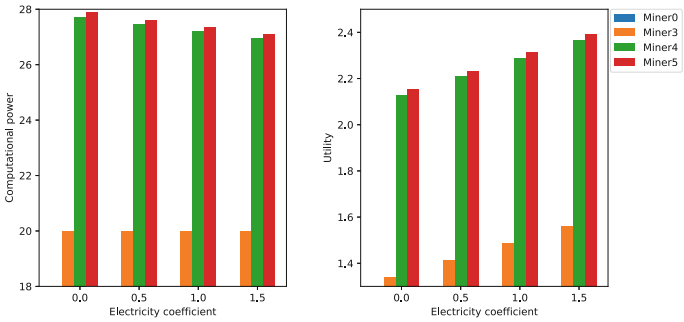

Fig. 4. Computational power and utility with different c_e

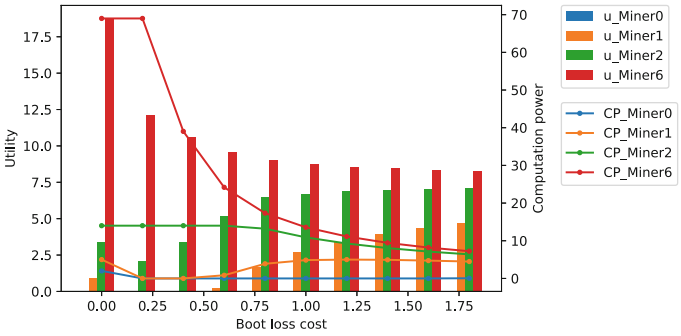

Fig. 5. Computational power and utility with different c_f

computational powers because it costs little to turn on rigs. However, when the cost gets larger, miners with few computation powers quit the game because the cost and others' computational powers are larger, while those who have medium computation powers still contribute all powers. But, players with higher power limitations decrease the powers due to the increment of boot loss cost as the lines in Fig. 5 show. When the costs keep increasing, players with more computational powers cut down the contributions because it cost more, while miners with fewer computational powers are likely to put more because the total computational powers are less than before and hence they have higher probabilities to gain rewards. As for the utility, miners with less computational powers gain more rewards while miners with more computational powers gain fewer rewards with the increase of boot loss cost.

As for the fixed assets depreciation cost c_r, there are three different situations as Fig. 6 shows. Miners with few computational powers as the $1st$ miner and the $2nd$ miner decrease their contributions when c_r exceeds a certain value because the cost has the most impact on these miners. Meanwhile, their utilities go down not only because the cost increases but also because players with higher limitations are likely to put more computational powers reducing their competitiveness. Miners with medium computational powers as the $4th$ miner

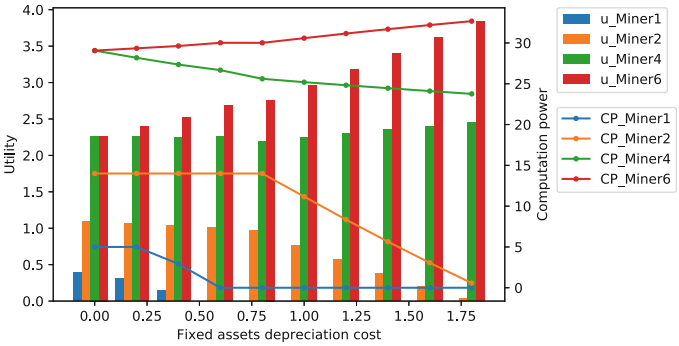

Fig. 6. Computational power and utility with different c_r

contributes less with the growth of c_r. However, the utility firstly goes down and then goes up. At first, the total computational powers decrease slowly since miners such as $2nd$ miner still participate in the game, and therefore the cost is the main effect on utility. Then when more and more miners give up, they are more possible to become the new DS committee member and hence their utilities rise up. As for the miners with much more computational powers as $6th$ miner, they have a higher willingness to contribute more computational powers and they gain more as well because they are less affected by high c_r than others.

6 Related Work

Sharding protocols are used in distributed databases [6,11] to achieve higher performance in which nodes are reliable at first. Then George Danezis and Sarah Meiklejohn [7] applied such ideas to a permissioned blockchain system which provides strong transparency and auditability guarantees for the central bank. Then,*ELASTICO* [15] was proposed later for a permissionless blockchain where miners are not trusted. However, the sharded permissionless blockchain framework in *ELASTICO* lacks details of rules for partitions and it only supports network sharding and transaction sharding ignoring stage sharding. OmniLedger [13] and RapidChain [25] supports stage sharding which allows miners to keep the part of the blockchain instead of the whole chain to save individual storage room. OmniLedge [13] also came up with an identity blockchain to record committees information while RapidChain [25] recommended reference committee instead.

Game theory has been widely used in blockchain systems especially the analysis of incentive and security. Some work [3,22] formulates the individual mining process in Bitcoin facing different rewards mechanisms, while some [14] study miners' investment strategies in mining pools. As for the security, most work focus on *selfish mining* where miners might break the rule to maximize their utilities. For example, Y. Zhen et al. [26] consider the situation when miners do not publish the block as soon as possible but hold them for higher utilities. Fork

chain selections are studied in [3,10,14]. However, all these work only consider the blockchain without shard which is not able to apply to sharded blockchains directly.

There is few work about game models in blockchain with shards. The work [16] firstly analyzed miners' behaviours in a sharded blockchain and came up with incentive mechanisms to motivate miners to participate in the system. However, it only considers the sharded blockchain system with one-layer committees such as ELASTICO. A cooperative game is formulated in [2] to form shards, which is not suitable in a PoW competition blockchain system. Zhengwei Ni [20] et al. model the consensus provision at the node level for multiple blockchains with shard as an evolutionary game which focus on sharded blockchain applications rather than itself.

7 Conclusion

In this paper, we have investigated the committee selection in a permissionless sharded blockchain with two-layer committees. We model the system as a hierarchy two-stage game model including the DS committee selection sub-game and shards formation sub-game and prove the existence of Nash equilibrium in both sub-games and the uniqueness of the DS committee selection sub-game. Then, we evaluate the game under different system parameters and the experimental results have illustrated that miners with higher computational power limitations are likely to contribute more powers to the game. It also shows that miners with high computational powers are more resistant to fixed assets depreciation cost than others, but they are more sensitive to boot loss cost.

Acknowledgement. This work was supported in part by the National Natural Science Foundation of China under Grant No. 61701216, Shenzhen Science, Technology and Innovation Commission Basic Research Project under Grant No. JCYJ20180507181527806, Guangdong Provincial Key Laboratory (Grant No. 2020B121201001) and "Guangdong Innovative and Entrepreneurial Research Team Program" (2016ZT06G587) and the"Shenzhen Sci-Tech Fund" (KYTDPT20181011104007).

References

1. The Zilliqa Project (2017). https://zilliqa.com
2. Asheralieva, A., Niyato, D.: Reputation-based coalition formation for secure self-organized and scalable sharding in IoT blockchains with mobile-edge computing. IEEE Internet Things J. **7**(12), 11830–11850 (2020)
3. Carlsten, M., Kalodner, H., Weinberg, S.M., Narayanan, A.: On the instability of bitcoin without the block reward. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 154–167 (2016)
4. Castro, M., Liskov, B., et al.: Practical byzantine fault tolerance. In: OSDI 1999, pp. 173–186 (1999)
5. Chiu, J., Koeppl, T.: Incentive compatibility on the blockchain. In: Trockel, W. (ed.) Social Design. SED, pp. 323–335. Springer, Cham (2019). https://doi.org/10.1007/978-3-319-93809-7_20

6. Corbett, J.C., et al.: Spanner: Google's globally distributed database. ACM Trans. Comput. Syst. (TOCS) **31**(3), 1–22 (2013)
7. Danezis, G., Meiklejohn, S.: Centrally banked cryptocurrencies. arXiv preprint arXiv:1505.06895 (2015)
8. Dhamal, S., Chahed, T., Ben-Ameur, W., Altman, E., Sunny, A., Poojary, S.: A stochastic game framework for analyzing computational investment strategies in distributed computing with application to blockchain mining. arXiv preprint arXiv:1809.03143 (2018)
9. Dimitri, N.: Bitcoin mining as a contest. Ledger **2**, 31–37 (2017)
10. Eyal, I.: The miner's dilemma. In: 2015 IEEE Symposium on Security and Privacy, pp. 89–103. IEEE (2015)
11. Glendenning, L., Beschastnikh, I., Krishnamurthy, A., Anderson, T.: Scalable consistency in scatter. In: Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles, pp. 15–28 (2011)
12. Han, Z., Niyato, D., Saad, W., Baar, T., Hjrungnes, A.: Game Theory in Wireless and Communication Networks: Theory, Models, and Applications, 1st edn. Cambridge University Press, Cambridge (2012)
13. Kokoris-Kogias, E., Jovanovic, P., Gasser, L., Gailly, N., Syta, E., Ford, B.: OmniLedger: a secure, scale-out, decentralized ledger via sharding. In: 2018 IEEE Symposium on Security and Privacy (SP), pp. 583–598. IEEE (2018)
14. Kroll, J.A., Davey, I.C., Felten, E.W.: The economics of bitcoin mining, or bitcoin in the presence of adversaries. In: Proceedings of WEIS, vol. 2013, p. 11 (2013)
15. Luu, L., Narayanan, V., Zheng, C., Baweja, K., Gilbert, S., Saxena, P.: A secure sharding protocol for open blockchains. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 17–30 (2016)
16. Manshaei, M.H., Jadliwala, M., Maiti, A., Fooladgar, M.: A game-theoretic analysis of shard-based permissionless blockchains. IEEE Access **6**, 78100–78112 (2018)
17. Nakamoto, S.: A peer-to-peer electronic cash system (2008). https://bitcoin.org
18. Nash, J.: Non-cooperative games. Ann. Math. 286–295 (1951)
19. Nayak, K., Kumar, S., Miller, A., Shi, E.: Stubborn mining: generalizing selfish mining and combining with an eclipse attack. In: 2016 IEEE European Symposium on Security and Privacy (EuroS&P), pp. 305–320. IEEE (2016)
20. Ni, Z., Wang, W., Kim, D.I., Wang, P., Niyato, D.: Evolutionary game for consensus provision in permissionless blockchain networks with shards. In: ICC 2019–2019 IEEE International Conference on Communications (ICC), pp. 1–6. IEEE (2019)
21. Sapirshtein, A., Sompolinsky, Y., Zohar, A.: Optimal selfish mining strategies in bitcoin. In: Grossklags, J., Preneel, B. (eds.) FC 2016. LNCS, vol. 9603, pp. 515–532. Springer, Heidelberg (2017). https://doi.org/10.1007/978-3-662-54970-4_30
22. Tsabary, I., Eyal, I.: The gap game. In: Proceedings of the 2018 ACM SIGSAC conference on Computer and Communications Security, pp. 713–728 (2018)
23. Wood, G.: Ethereum: a secure decentralised generalised transaction ledger (2014). https://ethereum.org
24. Yates, R.D.: A framework for uplink power control in cellular radio systems. IEEE J. Sel. Areas Commun. **13**(7), 1341–1347 (1995)
25. Zamani, M., Movahedi, M., Raykova, M.: Rapidchain: scaling blockchain via full sharding. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pp. 931–948 (2018)
26. Zhen, Y., Yue, M., Zhong-yu, C., Chang-bing, T., Xin, C.: Zero-determinant strategy for the algorithm optimize of blockchain pow consensus. In: 2017 36th Chinese Control Conference (CCC), pp. 1441–1446. IEEE (2017)