Cooperative Mining in Blockchain Networks With Zero-Determinant Strategies

Changbing Tang, *Member, IEEE*, Chaojie Li, *Member, IEEE*, Xinghuo Yu, *Fellow, IEEE*, Zhonglong Zheng, *Member, IEEE*, and Zhongyu Chen

***Abstract*—In proof-of-work (PoW)-based blockchain networks, the miners contribute their distributed computation in solving a crypto-puzzle competition to win the reward. To secure stable profits, some miners organize mining pools and share the rewards from the pool in proportion to each miner's contribution. However, some miners may exhibit malicious behaviors which cause a waste of distributed computation resource, even posing a threat on the efficiency of blockchain networks. In this paper, we propose a new game-theoretic framework to incentivize miners mining honestly and help to bring about a higher total welfare of blockchain networks. We first formulate the mining process as a noncooperative iterated game. We then propose a mechanism in terms of zero-determinant strategies (ZD strategies) to encourage the cooperative mining and improve the efficiency of mining in PoW-based blockchain networks. In addition, we theoretically analyze the maximum system welfare of the target pool through the method of optimization. Numerical illustrations are also presented to support our theoretical results.**

***Index Terms*—Blockchain networks, cooperative mining, game theory, zero-determinant strategies (ZD strategies).**

I. Introduction

The proof-of-work (PoW)-based blockchain network is a new paradigm of distributed computation system where participants contribute their computational resources in exchange for financial rewards, such as bitcoin. As the most successful application of blockchain technology, the core security of bitcoin relies on a PoW consensus algorithm and requires miners solving crypto-puzzles in the form of a hash computation [1]. During the process of mining, the difficulty of block generation is adjusted automatically, such that one block is created every 10 min to the blockchain [2]. Practically, it is impossible for a single miner using a small computational power to mine a block for years [3]. Consequently, miners often resort themselves into mining pools to secure a stable profit, where all members mine simultaneously and share their revenue whenever one of them creates a block.

However, the mining process of blockchain is very resource-intensive, which results in an intense competition and various dishonest mining strategies among miners [4]. A typical example is the block withholding (BWH) attack, where the infiltrating miners from other pools only submit partial PoWs (PPoWs) to the target pool as the computational share. The attacker will not change the pool's effective mining power [5]. Yet, the revenue of the attacked pool is shared with more miners, which gives rise to the fact that each miner earns less compared to the solo mining mode or the honest pool participation mode. Consequently, such an attack makes the pool reward system unfair by letting malicious miners receive unearned rewards, and even threaten the efficiency of the bitcoin system greatly. Therefore, it is necessary to design an effective and fair mechanism to make miners accountable for any dishonest mining behaviors and, thereby, enable efficient distributed computation of blockchain networks.

To address the challenge, a solution to prevent unfair supervisors and lazy miners from cheating has been investigated [6], where the technique can be applied to preventing misbehaving miners in the pool of blockchain networks. In addition, game theory is a promising theoretic tool for dealing with the problem of distributed optimization [7], [8], which results in subsequent efforts that have tried to align game theory to investigate distributed computational problems [5]. For example, the dynamics of mining pool selection in a blockchain network has been studied from the view of evolutionary game [9]. Moreover, a game theoretical model has been employed to show distributed computation in analyzing the security of pool protocols [10]. However, how to conduct mining effectively in the blockchain network has not been fully considered where an optimization problem can be formulated.

Recently, a new class of probabilistic and conditional strategies in game theory has emerged, which are referred to as zero-determinant strategies (ZD strategies) [11]. The ZD strategies are employed in the iterated game to deal with the competition of two-player games [12], [13] and multiplayer games [14]–[16]. Furthermore, there are several applications of ZD strategies in competition and cooperation problems. For example, Zhang *et al.* applied ZD strategies in wireless communication for the cooperation of resource sharing in [17] and [18]. Daoud *et al.* [19] formulated secondary sharing of the wireless spectrum as an iterated game and applied ZD strategies to achieve any feasible outcome. Regardless of the strategy of its opponents, the player with ZD strategies is capable of unilaterally setting a ratio between the players and their opponents' expected payoff. We thus propose a mechanism in terms of ZD strategies to prevent misbehaving miners in the pool of blockchain networks, in which the social welfare of the system is optimized.

In this paper, we develop a theory of multiplayer ZD strategies and study the problem of cooperative mining in a PoW-based blockchain network from the viewpoint of game theory. The problem is challenging due to several reasons. First, each miner is associated with certain private information which is unknown for other workers. Second, miners' decisions are coupled with each other, which results from one miner's choice affecting other miners' payoffs. Third, the interactions among miners are multiple, and all rational miners maximize

Manuscript received October 16, 2018; revised February 24, 2019; accepted April 26, 2019. Date of publication May 22, 2019; date of current version September 23, 2020. This work was supported in part by the National Natural Science Foundation of China under Grant 61751303, Grant 61672467, Grant 61672468, Grant 11572288, and Grant 61877055, in part by the Zhejiang Provincial Natural Science Foundation of China under Grant LY16F030002, and in part by the Australian Research Council Discovery Program under Grant DP170102303. This paper was recommended by Associate Editor B. Sick. *(Corresponding author: Changbing Tang.)*

C. Tang is with the College of Physics and Electronics Information Engineering, Zhejiang Normal University, Jinhua 321004, China, and also with the School of Engineering, RMIT University, Melbourne, VIC 3001, Australia (e-mail: tangcb@zjnu.edu.cn).

C. Li is with Aliexpress, Alibaba Group, Hangzhou 311100, China (e-mail: cjlee.cqu@163.com).

X. Yu is with the School of Engineering, RMIT University, Melbourne, VIC 3001, Australia (e-mail: x.yu@rmit.edu.au).

Z. Zheng and Z. Chen are with the College of Mathematics and Computer Science, Zhejiang Normal University, Jinhua 321004, China (e-mail: zhonglong@zjnu.edu.cn; czy@zjnu.edu.cn).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCYB.2019.2915253

their own interests, which makes it difficult for miners to achieve equilibria with honest mining during repeated interactions without complete information.

In this paper, we first formulate the mining process as an iterated game where all miners in the target pool solve a crypto-puzzle to win the reward. Second, we propose a method in terms of ZD strategies aiming to optimize the efficiency of the blockchain network, which serves to incentivize the cooperative mining of miners. Last, we obtain the theoretical solution of the maximum system welfare through solving an optimization problem. The main contributions of this paper are summarized as follows.

1) *Novel Model:* We model the mining process with a group of miners solving a crypto-puzzle as an iterated multiplayer game, which allows competitive and self-organized miners making decisions for their own to address the problem of cooperative mining in the PoW-based blockchain network.
2) *New Optimized Method:* We propose an incentive scheme in terms of ZD strategies to incentivize miners mining honestly from the viewpoint of optimization, in which the maximum welfare of the blockchain network can be achieved.
3) *Theoretical and Practical Insights:* Our analysis helps us to understand how different miners choose their strategies to enable the welfare of a blockchain system at a high level. Furthermore, our analysis provides a clue for designing a new consensus algorithm of a blockchain system, where the high efficient distributed computation is achieved spontaneously.

The rest of this paper is organized as follows. Section II reviews the literature on this topic. Section III describes the system model and formulates the mining process as a noncooperative iterated game. In Section IV, we propose a mechanism in terms of ZD strategies to encourage cooperative mining and improve the efficiency of mining in PoW-based blockchain networks, in which the condition of the maximum system welfare is analyzed. In Section V, numerical simulations are carried out for the proposed ZD strategies. Finally, the conclusions are stated in Section VI.

II. Related Work

In the literature, several works have focused on the study of the pool game based on game theory. For instance, Eyal qualitatively analyzed the Nash equilibrium (NE) of the mining game and gave the existence conditions of the NE for any number of pools [5]. In [3], the choice of miners was transformed into a cooperative game model, in which the members of the same pool were regarded as an alliance. In [9], the evolutionary games were used to study the dynamics of mining pool selection in a blockchain network, where mining pools may choose arbitrary block mining strategies. In addition, the blockchain bifurcation loophole was applied to map the mining model into a random game with complete information [20]. Furthermore, Johnson *et al.* [21] employed a series of game-theoretical models to explore the tradeoff of DDoS attacks between two pools, and found that pools have a greater incentive to attack large pools than small ones. However, how to conduct mining effectively with game theory in the blockchain network has not been fully considered.

Recently, ZD strategies, as a new method in game theory, have been applied to study the mining problem of PoW-based blockchain networks. For instance, in our previous work, we analyzed the existence conditions of the NE and applied ZD strategies to study the strategies selection during the PoW consensus process [22]. Moreover, we modeled a mining process with two miners as an iterated game and proposed a subclass of a ZD strategy to alleviate miners' dilemma in PoW-based blockchain networks [23]. In addition, in [24], an adaptive ZD strategy was proposed to promote the cooperation of miners between two pools in the process of pool mining.

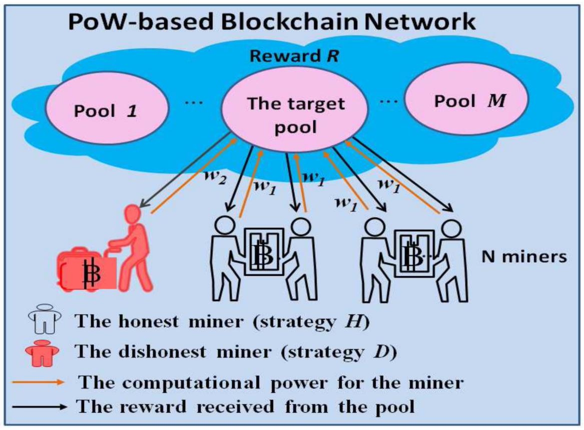
PoW-based Blockchain Network
Reward R
Pool 1
...
The target pool
...
Pool M
w_2
w_1
w_1
w_1
w_1
N miners
The honest miner (strategy H)
The dishonest miner (strategy D)
The computational power for the miner
The reward received from the pool

Fig. 1. PoW-based blockchain network, in which pool miners contribute their computational resources in exchange for financial rewards R. There are N miners in the target pool, where each miner has two strategies: H (honest mining) and D (malicious mining). The honest miner joins the pool with a hash rate w_1, the dishonest miner joins the pool with a hash rate w_2, and the total hash rate of other pools is w.

In this paper, we focus on optimization of mining efficient from the viewpoint of game theory using multiplayer ZD strategies. This paper is different from the previous studies in the following aspects. First, we model the mining process as a noncooperative iterated multiplayer game, in which the interactions among miners are multiple. We capture the scenario of repeated multi-interactions for the mining process as an iterated quasi-public goods game (quasi-PGG) [25]. This is different from previous studies in [22]–[24], where the interaction of game model with two-player was studied and cannot reflect the practical complex situation among multiple players. Second, we develop a theory of multiplayer ZD strategies from the viewpoint of optimization, in which the optimization of system welfare is achieved spontaneously from bottom to top. This is also different from [22]–[24], where the focus was on cooperation of miners and dynamics of strategies.

III. System Model

We consider a PoW-based blockchain network where each pool generated by different miners solves a crypto-puzzle competition to win the reward. According to the Nakamoto consensus protocol [1], only the first pool that accomplishes the PoW will be rewarded. Thus, we pay attention to the computational competition of the target pool who is the winner in a certain turn of the crypto-puzzle solving.

As illustrated in Fig. 1, we consider that there are N miners in the target pool. As we known, the resource of PoW computation is consumable while the computational competition is intense, which results in fact that a part of miners present a dishonest mining strategy during the competition mining process. Consider the competitive computation as the computational power of miners which provides to the target pool. Thus, we assume that there are two choices for miners in the pool: H and D, where H means miner with honest strategy (cooperative mining) and D means miner mining with dishonest strategy (malicious mining). Notably, the probability of the pool winning the reward is positively proportional to the available computational power of the pool. If all miners act malicious behaviors, they will probably get nothing. Therefore, there are strategies choosing for all miners who act strategically to maximize their own profits during the mining process. This similarity leads to a strong mapping between elements of mining process in the PoW-based blockchain network and game theoretical components.

Definition 1: A mining game $\mathbb{G}$ in PoW-based blockchain network is triple $(I, \mathbb{A}, U)$, where:

1) $I = \{1, 2, \dots, N\}$ denotes the set of players;
2) $\mathbb{A} = (a_1, \dots, a_k, \dots, a_N)$ is the strategy profile of all workers and $a_k \in \{H, D\}$ is the strategy of player k;
3) U presents the realized payoffs and u^k presents the payoff of player k.

There are two components of the block reward, that is, a fixed token-issuing reward and the fees of the transactions packed in the block [26]. Let L be the current block size. R is the token-issuing reward and σ is the transaction confirmation price per unit data size. The transaction fees can be expressed as σL [27]. Furthermore, the energy cost of hash computation is also considered for all miners. Let λ be the energy price for maintaining a unit hash rate during one block process, and n $(n \in \{0, 1, 2, \dots, N\})$ be the honest miners in the target pool. Assume the honest miner joins the pool with a hash rate w_1, while the dishonest miner joins the pool with a hash rate w_2. Here, the dishonest miner only provides partial computational power for the target pool, which results in $w_2 \ll w_1$. Let w be the total hash rate of other pools. Thereby, the probability for the target pool to win the reward is

$$P^{\text{win}} = \frac{nw_1 + (N-n)w_2}{nw_1 + (N-n)w_2 + w}.$$

At last, the reward is shared among all N workers which is positively proportional to the available computational power of the miners provided. On the other hand, a miner will cost a high mount λw_1 with strategy H; while he will cost a low mount λw_2 with strategy D. Concretely, if the miner k adopts with strategy H (D) in a certain turn of the game, his expected payoff will be

$$\begin{cases} u^k_{H,n} = \frac{R+\sigma L}{N} \cdot P^{\text{win}} \cdot \frac{nw_1}{nw_1+(N-n)w_2} - \lambda w_1 \\ u^k_{D,n} = \frac{R+\sigma L}{N} \cdot P^{\text{win}} \cdot \frac{(N-n)w_2}{nw_1+(N-n)w_2} - \lambda w_2. \end{cases} \tag{1}$$

Since $w_2 \ll w_1$, the probability P^{win} mainly depends on the number of honest miners n and the hash rate of honest miner w_1. Thus, increasing the number of the honest miner n will greatly enhance the expected payoff of each miner together with the social welfare of the target pool when the hash rate is fixed. In addition, the dishonest miner acts as a spoiler who will threaten the benefit of the target pool. This phenomenon is similar with "tragedy of the commons" of PGG, where the free riders contribute less but share the final reward [25]. Under the framework of game theory, the honest miners cannot win in a single-round game. Fortunately, the situation is changed if the miners interact repeatedly. Since the mining is a persistent process, we then capture the scenario of repeated interactions for the mining process as an iterated quasi-PGG, in which each miner needs to consider effects of his action at any round of the game on the future feedback of the other miners.

IV. Cooperative Mining With ZD Strategies

It is known that the long-memory player has no advantage over the short-memory player when each stage game is identically repeated infinite times [11]. Thus, we assume all miners have memory of only one previous move, that is, all miners' strategies taken in the current round only depend on the outcome of the previous round. In this paper, we focus on miners who only consider their own action in the previous round and the number of honest miners. That is, the miners do not know the co-miners' strategies during the mining process. After finishing one round of the game, the outcome of game, such as the number of honest miners, can be observed by the system manager.

For N-miner two-strategy games, there are 2^N possible outcomes in each round. We use a mixed strategy $\mathbf{s^k}$ to express the conditional probabilities for the cooperative mining as regards every possible outcome for the miner k $(k \in \{1, 2, \dots, N\})$. Especially, the mixed strategy is a 2^N-dimensional vector

$$\mathbf{s^k} = \left[s^k_1, \dots, s^k_i, \dots, s^k_{2^N}\right]^T \tag{2}$$

where s^k_i represents the conditional probability for the miner k with honest strategy in the current round conditioned on the ith outcome of the previous round.

Denote the number of miners with H among the opponents of miner k in the last round as m $(m \in \{0, 1, \dots, N-1\})$. Note that if miner k adopts strategy H, then $m = n - 1$; while miner k adopts strategy D, then $m = n$. If the previous action of the miner k is H (or D), the probability of his adopting H in the current round is $s_{H,m}$ (or $s_{D,m}$). Assume that the game is symmetric, such that payoffs do not depend on which miners are honest, but on how many honest miners [14]. In such a scenario, the vector $\mathbf{s^k}$ in (2) can be represented by a 2^N-dimensional vector with $2N$ independent variables as

$$\begin{aligned} \mathbf{s}^k = \Big[&s^k_{H,0}, \dots, s^k_{H,m}, \dots, s^k_{H,m}, \dots, s^k_{H,N-1} \\ &s^k_{D,0}, \dots, s^k_{D,m}, \dots, s^k_{D,m}, \dots, s^k_{D,N-1}\Big]^T. \end{aligned} \tag{3}$$

It is noticed that there are $\binom{N-1}{m}$ terms of $s^k_{H,m}$ and $s^k_{D,m}$, which leads to that the number of independent variable reduces to $2N$. Taking $N = 3$ as an example, there are 2^3 possible outcomes. That is $\{HHH, HHD, HDH, HDD, DHH, DHD, DDH, DDD\}$, which results in that $\mathbf{s^k} = [s^k_{H,2}, s^k_{H,1}, s^k_{H,1}, s^k_{H,0}, s^k_{D,2}, s^k_{D,1}, s^k_{D,1}, s^k_{D,0}]^T$. Here, both the second and the third elements are $s^k_{H,1}$ which corresponds to the outcomes that miner k takes strategy H while exactly one of his opponents take strategy H, that is, the element $s^k_{H,1}$ corresponds to the outcomes HHD and HDH. Similarly, the element $s^k_{D,1}$ corresponds to the outcomes DHD and DDH. Thus, the mixed strategy vector $\mathbf{s^k}$ of miner k can be expressed with six independent variables, that is, $s^k_{H,j}$, and $s^k_{D,j} (j = 0, 1, 2)$.

Similarly, the payoff vector $\mathbf{U}^k$ of the miner k can be represented by

$$\begin{aligned} \mathbf{U}^k = \Big[&u^k_{H,0}, \dots, u^k_{H,m}, \dots, u^k_{H,m}, \dots, u^k_{H,N-1} \\ &u^k_{D,0}, \dots, u^k_{D,m}, \dots, u^k_{D,m}, \dots, u^k_{D,N-1}\Big]^T \end{aligned} \tag{4}$$

where there are $\binom{N-1}{m}$ terms of $u^k_{H,m}$ and $u^k_{D,m}$.

On the other hand, the multiminer game can be characterized by a Markov chain with a state transition matrix $\mathbf{M} = [q_{ij}]_{2^N \times 2^N}$ [14], where q_{ij} represents the probability of transition from the previous state i to the current state j. For a state HHD when $N = 3$ as an example, the conditional probabilities that the miners 1, 2, and 3 select H (or D) in the current round are $s^1_{H,1}$, $s^2_{H,1}$, and $s^3_{D,2}$, respectively. Therefore, the probability q_{23} of transition from the previous state HHD to the current state HDH equals $s^1_{H,1}(1 - s^2_{H,1})s^3_{D,2}$. Define a matrix $\mathbf{M}' \equiv \mathbf{M} - \mathbf{I}$, where $\mathbf{I}$ is the identity matrix. If the transition matrix $\mathbf{M}$ is regular, it will ensure that there is a stationary vector $\mathbf{v}$, such that $\mathbf{v^T} \cdot \mathbf{M} = \mathbf{v^T}$ and $\mathbf{v^T} \cdot \mathbf{M}' = \mathbf{0}$ [11]. Assume $\mathbf{f}$ is the last column of $\mathbf{M}'$. Then, we get the equation

$$\mathbf{v^T} \cdot \mathbf{f} = \det\Big(\mathbf{s^1}, \dots, \mathbf{s^k}, \dots, \mathbf{f}\Big)$$

where $(\mathbf{s^1}, \dots, \mathbf{s^k}, \dots, \mathbf{f})$ is a $2^N \times 2^N$ matrix. Replacing $\mathbf{f}$ with $\theta_1 \mathbf{U^1} + \sum_{k=2}^{N} \theta_k \mathbf{U^k} - \gamma \mathbf{1}$ by using the Laplace expansion, we can get a linear combination of all the miners' expected payoffs with the following equation:

$$\theta_1 E^1 + \sum_{k=2}^{N} \theta_k E^k - \gamma = \frac{\det\left(\mathbf{s^1}, \ldots, \mathbf{s^k}, \ldots, \theta_1 \mathbf{U^1} + \sum_{k=2}^{N} \theta_k \mathbf{U^k} - \gamma \mathbf{1}\right)}{\det\left(\mathbf{s^1}, \ldots, \mathbf{s^k}, \ldots, \mathbf{1}\right)} \tag{5}$$

where E^k is the expected payoff of worker k; γ is a scalar; and $\theta_k (k \in \{1, 2, \ldots, N\})$ are the weight factors of payoff function $\mathbf{U}^k$.

In the mining process, if the miner k_0 selects $\mathbf{s}^{k_0}$ properly (denoted as $\widetilde{\mathbf{s}}^{k_0}$) which satisfies

$$\widetilde{\mathbf{s}}^{k_0} = \psi\left(\theta_1 \mathbf{U}^{k_0} + \sum\nolimits_{k=1, k\neq k_0}^{N} \theta_k \mathbf{U^k} - \gamma \mathbf{1}\right) \tag{6}$$

where ψ ($\psi \neq 0$) is a coefficient, then the miner k_0 can unilaterally enforce a linear relationship between each miner's excepted payoff, that is,

$$\theta_1 E^1 + \sum\nolimits_{k=1, k\neq k_0}^{N} \theta_k E^k - \gamma = 0. \tag{7}$$

We call these linear combinations of miners' payoff vectors as ZD strategies whose definition results from $\det(\mathbf{s^1}, \ldots, \mathbf{s^k}, \ldots, \mathbf{f}) = 0$. Note that the $\widetilde{\mathbf{s}}^{k_0}$ is the last column of $\mathbf{M}'$, which is determined by $\mathbf{s}^{k_0}$. Concretely, we denote it as

$$\widetilde{\mathbf{s}}^{k_0} = \left[-1 + s_{H,0}^{k_0}, \ldots, -1 + s_{H,N-1}^{k_0}, s_{D,0}^{k_0}, \ldots, s_{D,N-1}^{k_0}\right]. \tag{8}$$

Define the total expected payoff of all miners as the system welfare, that is, $E_{\text{sys}} = \theta_1 E^1 + \sum_{k=1, k\neq k_0}^{N} \theta_k E^k$. According to (7), we know that when the miner takes the ZD strategy regardless of the behavior of other miners, he can pin the total excepted payoff of all his opponents at a desired level, that is, $\gamma = E_{\text{sys}}$. Thus, the maximum and stable system welfare can be achieved by solving the following optimization:

$$\begin{aligned} \max_{s_{H,m}^{k_0}, s_{D,m}^{k_0}} \quad & \gamma \\ \text{s.t.} \quad & \begin{cases} 0 \leq s_{H,m}^{k_0}, \quad s_{D,m}^{k_0} \leq 1 \\ \widetilde{\mathbf{s}}^{k_0} = \psi\left(\theta_1 \mathbf{U^1} + \sum_{k=1, k\neq k_0}^{N} \theta_k \mathbf{U^k} - \gamma \mathbf{1}\right). \end{cases} \end{aligned} \tag{9}$$

Lemma 1: In multiminer mining game, the optimization problem of (9) exists a feasible solution when the miner k_0 takes the ZD strategy $\widetilde{\mathbf{s}}^{k_0} = \psi(\theta_1 \mathbf{U^1} + \sum_{k=1, k\neq k_0}^{N} \theta_k \mathbf{U^k} - \gamma \mathbf{1})$.

Proof: When $\widetilde{\mathbf{s}}^{k_0} = \psi(\theta_1 \mathbf{U^1} + \sum_{k=1, k\neq k_0}^{N} \theta_k \mathbf{U^k} - \gamma \mathbf{1})$, according to (7), we have $\gamma = E_{\text{sys}}$. Note that $\widetilde{\mathbf{s}}^{k_0} = [-1 + s_{H,0}^{k_0}, \ldots, -1 + s_{H,N-1}^{k_0}, s_{D,0}^{k_0}, \ldots, s_{D,N-1}^{k_0}]$, then

$$\begin{cases} s_{H,m}^{k_0} = 1 + \psi\left(\theta_1 U_{H,m}^1 + \sum_{\substack{k=1 \\ k\neq k_0}}^{N} \theta_k U_{H,m}^k - \sum_{k=1}^{N} \theta_k E^k\right) \\ s_{D,m}^{k_0} = \psi\left(\theta_1 U_{D,m}^1 + \sum_{\substack{k=1 \\ k\neq k_0}}^{N} \theta_k U_{D,m}^k - \sum_{k=1}^{N} \theta_k E^k\right). \end{cases} \tag{10}$$

Denote $W_H(m) = \theta_1 U_{H,m}^1 + \sum_{k=1, k\neq k_0}^{N} \theta_k U_{H,m}^k$ and $W_D(m) = \theta_1 U_{D,m}^1 + \sum_{k=1, k\neq k_0}^{N} \theta_k U_{D,m}^k$, respectively. When $\psi > 0$, since $0 \leq s_{H,m}^k \leq 1$ and $0 \leq s_{D,m}^k \leq 1$, then we obtain

$$\begin{cases} -1 \leq \psi\left(W_H(m) - \theta_1 E^1 - \sum_{k=1, k\neq k_0}^{N} \theta_k E^k\right) \leq 0 \\ 0 \leq \psi\left(W_D(m) - \theta_1 E^1 - \sum_{k=1, k\neq k_0}^{N} \theta_k E^k\right) \leq 1. \end{cases} \tag{11}$$

Through some mathematical derivation, we have

$$\begin{cases} \max\left\{W_H(m), -\frac{1}{\psi} + W_D(m)\right\} \leq \gamma \\ \gamma \leq \min\left\{W_D(m), W_H(m) + \frac{1}{\psi}\right\}. \end{cases} \tag{12}$$

When $\psi > 0$, $W_H(m) < W_H(m) + (1/\psi)$ and $-(1/\psi) + W_D(m) < W_D(m)$, which results in the inequality $\max(W_H(m), -(1/\psi) + W_D(m)) \leq \min(W_D(m), W_H(m) + (1/\psi))$. Therefore, there is a feasible domain of γ which satisfies

$$\max\left(W_H(m), -\frac{1}{\psi} + W_D(m)\right) < \gamma < \min\left(W_D(m), W_H(m) + \frac{1}{\psi}\right).$$

Similarly, when $\psi < 0$, we also have $\theta_1 E^1 + \sum_{k=1, k\neq k_0}^{N} \theta_k E^k \geq \max\{W_H(m) + (1/\psi), W_D(m)\}$ and $\theta_1 E^1 + \sum_{k=1, k\neq k_0}^{N} \theta_k E^k \leq \min\{W_D(m) - (1/\psi), W_H(m)\}$. There is also a feasible domain of γ which satisfies

$$\max\left\{W_H(m) + \frac{1}{\psi}, W_D(m)\right\} < \gamma < \min\left\{W_D(m) - \frac{1}{\psi}, W_H(m)\right\}.$$

■

Theorem 1: In the multiminer mining game, the miner k_0 can control the system welfare reached the maximum value, that is,

$$\gamma_{\max} = \begin{cases} \min\left\{W_D(m), W_H(m) + \frac{1}{\psi}\right\}, & \psi > 0 \\ \min\left\{W_D(m) - \frac{1}{\psi}, W_H(m)\right\}, & \psi < 0 \end{cases} \tag{13}$$

if the ZD strategy $\widetilde{\mathbf{s}}^{k_0} = \psi(\theta_1 \mathbf{U^1} + \sum_{k=2}^{N} \theta_k \mathbf{U^k} - \gamma \mathbf{1})$ is applied, where $W_H(m) = (\theta_2 + \cdots + \theta_{N-m}) \cdot u_{D,m+1}^k + (\theta_1 + \theta_{N-m+1} + \cdots + \theta_N) \cdot u_{H,m}^k$ and $W_D(m) = (\theta_1 + \theta_2 + \cdots + \theta_{N-m+1}) \cdot u_{D,m}^k + (\theta_{N-m+2} + \cdots + \theta_N) \cdot u_{H,m-1}^k$.

Proof: According to Lemma 1, we know that there is a feasible solution of γ under appropriate conditions. Then, we can obtain the $\gamma_{\max}$ from feasible solution. Based on the payoff (1), we can obtain $W_H(m) = (\theta_2 + \cdots + \theta_{N-m}) \cdot u_{D,m+1}^k + (\theta_1 + \theta_{N-m+1} + \cdots + \theta_N) \cdot u_{H,m}^k$, and $W_D(m) = (\theta_1 + \theta_2 + \cdots + \theta_{N-m+1}) \cdot u_{D,m}^k + (\theta_{N-m+2} + \cdots + \theta_N) \cdot u_{H,m-1}^k$. Thus, when $\psi > 0$, we can choose appropriate parameters to satisfy the feasible domain of γ and achieve the maximum value $\gamma_{\max} = \min\{W_D(m), W_H(m) + (1/\psi)\}$ which is independent with other miners' strategies. The similarity also fits for the case of $\psi < 0$, in which $\gamma_{\max} = \min\{W_D(m) - (1/\psi), W_H(m)\}$.

To summarize, when the miner takes the ZD strategy whatever the strategies of other miners are taken, the system welfare can be unilaterally maintained at the value of $\gamma_{\max}$ as shown in (13). ■

Remark 1: It is shown that $\gamma_{\max}$ is a linear combination of payoff $u_{H,m}^k$ and $u_{D,m}^k$ which rely on system parameters R, L, m, w_1, w_2, and w. In fact, R and L only have an influence on the value of $\gamma_{\max}$, while m, w_1, w_2, and w also affect the strategy selection of the miners, that is, the equilibria of the mining game.

V. Performance Evaluation

In this section, we illustrate the performance of the ZD strategies of the mining game with numerical analysis. To illustrate the effectiveness of our proposed scheme, we compare ZD strategies with other classical strategies, such as average strategy [28] $\mathbf{s} = [s_1, \ldots, s_i, \ldots, s_{2^N}]^T$ ($s_i = 0.5$ for all $i \in \{1, 2, \ldots, 2^N\}$); aggressive strategy [29] $\mathbf{s} = [s_1, \ldots, s_i, \ldots, s_{2^N}]^T$ ($s_i = 0$ for all $i \in \{1, 2, \ldots, 2^N\}$, i.e., attack all the time); energy-saving strategy [30] $\mathbf{s} = [s_1, \ldots, s_i, \ldots, s_{2^N}]^T$ ($s_i = 1$ for all $i \in \{1, 2, \ldots, 2^N\}$, i.e., cooperative mining all the time); win-stay-lose-shift (WSLS) strategy [31] (cooperate after mutual cooperation and mutual attack otherwise attack); and Tit-for-Tat [31] (cooperate if at least k co-miners cooperated in the previous round). Assume that the original

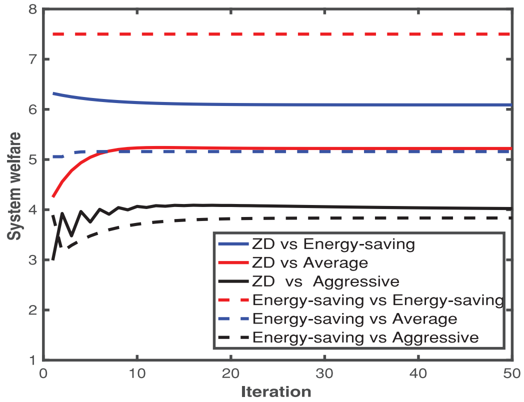

Fig. 2. Social welfare of ZD strategies versus energy-saving, average, and aggressive strategies when $N = 3$.

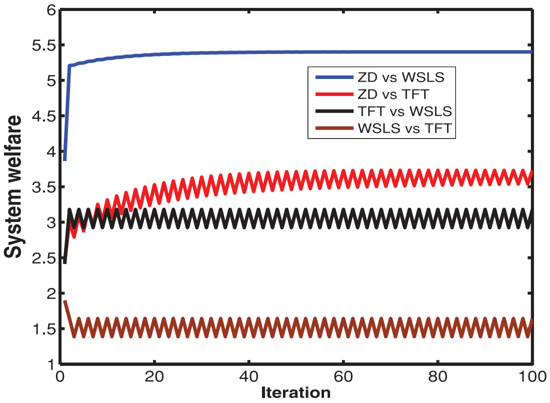

Fig. 3. Social welfare of ZD strategies versus TFT and WSLS strategies when $N = 3$.

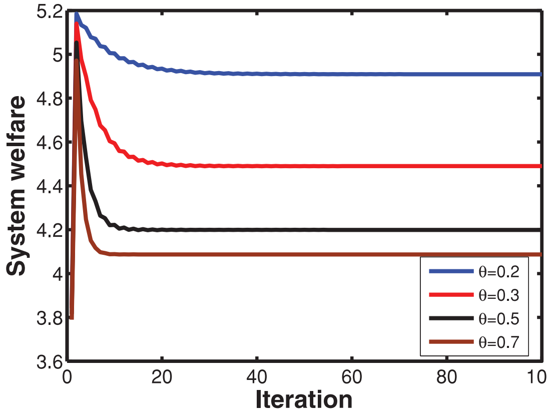

Fig. 4. Social welfare obtained by the miner takes the ZD strategy with different values of θ when $N = 3$.

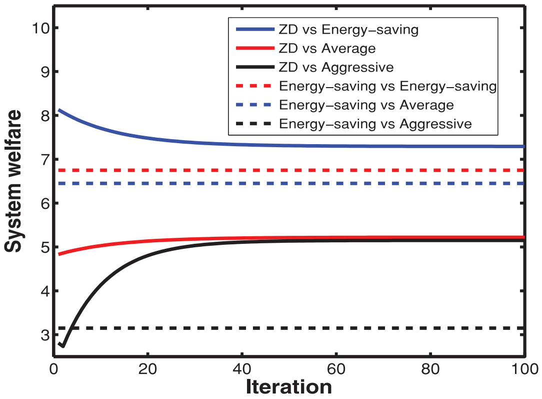

Fig. 5. Social welfare of ZD strategies versus energy-saving, average, and aggressive strategies when $N = 6$.

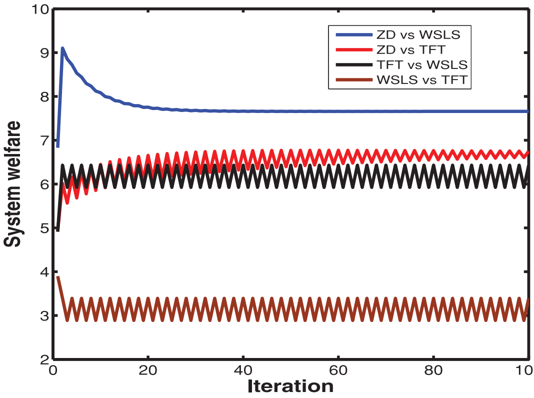

Fig. 6. Social welfare of ZD strategies versus TFT and WSLS strategies when $N = 6$.

probability of each states as $v^0 = [v_1^0, \ldots, v_i^0, \ldots, v_{2N}^0]^T$, where $v_i^0 = 0.125$ for all $i \in \{1, 2, \ldots, 2^N\}$.

We first consider the situation when $N = 3$. Set system parameters as $R = 7$, $\sigma = 0.5$, $L = 2$, $\lambda = 0.02$, $w_1 = 40$, $w_2 = 1$, $w = 5$, $\theta_1 = -0.1$, $\theta_2 = 0.2$, $\theta_3 = 0.2$, and $\psi = -0.5$. Let one miner adopts the ZD strategy whose $\widetilde{\mathbf{s}}^{k_0}$ satisfies (6). Fig. 2 shows that an energy-saving strategy facing energy-saving strategy can result in the highest system welfare, whose performance is better than the other strategies' performance. However, compared to the average-taking and the aggressive strategies, the miner taking the ZD strategy can always achieve the higher system welfare when facing an average-taking miner or an aggressive miner. In Fig. 3, we show that when the miner adopts the ZD strategy facing the WSLS opponents, the system welfare converges to a high and stable value at 5.27. However, when the miner adopts the TFT facing the WSLS opponents, the system welfare is fluctuated around 3. The similar situation occurs in the scene of the ZD strategy versus the TFT, in which the welfare with the ZD strategy is higher than that of welfare with the TFT strategy. While in Fig. 4, we show the effect of the weight factor on the social welfare. For convenience, we set $\theta_2 = \theta_3 = \theta$. We fix $\theta_1 = -0.1$ and vary the value of θ which satisfy (6) to show the effect on the performance of ZD strategies. It is shown that when the miner takes ZD strategies, the social welfare converges to stable values which decrease with the increasing of value θ.

In Figs. 5–7, we illustrate the performance of the ZD strategies when $N = 6$. In this case, we set parameters as $R = 10$, $\sigma = 0.5$, $L = 8$, $\lambda = 0.02$, $w_1 = 40$, $w_2 = 1$, $w = 5$, $\theta_1 = -0.1$, $\theta_2 = 0.2$, $\theta_3 = 0.1$, $\theta_4 = 0.2$, $\theta_5 = 0.2$, $\theta_6 = 0.1$, and $\psi = -0.5$. Let one miner adopt the ZD strategy whose $\widetilde{\mathbf{s}}^{k_0}$ satisfies (6). Fig. 5 shows that when the miner takes the energy-saving facing the energy-saving strategy or the average-taking strategy, the system welfare converges to 5.22 and 5.15, where the performance is better than that of performance with one miner takes the energy-saving facing aggressive strategy. Furthermore, when the miner takes the ZD strategy facing the energy-saving strategy, the system welfare can reach a high and stable value at 7.29. In Fig. 6, we show the performance of the ZD strategy versus the WSLS and TFT strategies, in which the performance of the ZD strategy is better than other strategies. We also show the effect of the weight factor on the social welfare in Fig. 7. Similarly, we set

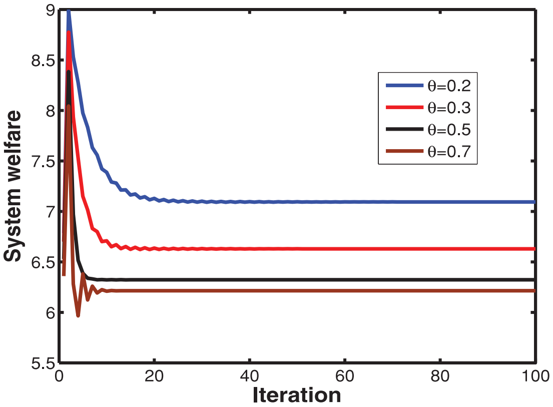

Fig. 7. Social welfare obtained by the miner takes the ZD strategy with different values of θ when $N = 6$.

$\theta_2 = \theta_3 = \theta_4 = \theta_5 = \theta_6 = \theta$. We fix $\theta_1 = -0.1$ and vary the value of θ. Here, parameters also satisfy (6). It is shown that the stable value of social welfare decreases with the increasing of value θ.

VI. Conclusion

In this paper, we have considered the problem of cooperative mining for the PoW-based blockchain network. We have modeled the process of mining as an iterated quasi-PGG which can be considered as a multitask consensus protocol among rational and selfish miners. Further, we have proposed the ZD-strategies-based mechanism to analyze the process of mining, in which the miner is able to maintain the system welfare at a desired value whatever the strategies of others are taking. Moreover, we have analyzed the maximum system welfare through solving an optimization problem. In addition, we have compared the proposed ZD strategies with other classical strategies in dealing with the cooperative mining problem by the numerical simulations.

Acknowledgment

The authors would like to thank the Editor and reviewers for a number of constructive comments and suggestions that have improved the quality of this paper.

References

[1] S. Nakamoto. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: http://www.bitcoin.org/bitcoin.pdf

[2] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity: Extending bitcoin's proof of work via proof of stake," *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 42, no. 3, pp. 34–37, Dec. 2014.

[3] Y. Lewenberg, Y. Bachrach, Y. Sompolinsky, A. Zohar, and J. S. Rosenschein, "Bitcoin mining pools: A cooperative game theoretic analysis," in *Proc. Int. Conf. Auton. Agents Multiagent Syst.*, Istanbul, Turkey, May 2015, pp. 919–927.

[4] Y. Kwon, D. Kim, Y. Son, E. Vasserman, and Y. Kim, "Be selfish and avoid dilemmas: Fork after withholding (FAW) attacks on bitcoin," in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, Dallas, TX, USA, Oct. 2017, pp. 195–209.

[5] I. Eyal, "The miner's dilemma," in *Proc. IEEE Symp. Security Privacy (SP)*, San Jose, CA, USA, May 2015, pp. 89–103.

[6] M. T. Goodrich, "Pipelined algorithms to detect cheating in long-term grid computations," *Theor. Comput. Sci.*, vol. 408, nos. 2–3, pp. 199–207, Nov. 2008.

[7] T. L. Vincent and T. L. S. Vincent, "Evolution and control system design. The evolutionary game," *IEEE Control Syst. Mag.*, vol. 20, no. 5, pp. 20–35, Oct. 2000.

[8] T. Basar, G. J. Olsder, *Dynamic Noncooperative Game Theory*, 2nd ed. Philadelphia, PA, USA: SIAM, 1999.

[9] X. J. Liu, W. B. Wang, D. Niyato, N. Zhao, and P. Wang, "Evolutionary game for mining pool selection in blockchain networks," *IEEE Wireless Commun. Lett.*, vol. 7, no. 5, pp. 760–763, Oct. 2018.

[10] L. Luu, R. Saha, I. Parameshwaran, P. Saxena, and A. Hobor, "On power splitting games in distributed computation: The case of bitcoin pooled mining," in *Proc. IEEE 28th Comput. Security Found. Symp.*, Verona, Italy, Jul. 2015, pp. 397–411.

[11] W. H. Press and F. J. Dyson, "Iterated prisoner's dilemma contains strategies that dominate any evolutionary opponent," *Proc. Nat. Acad. Sci. USA*, vol. 109, no. 26, pp. 10409–10413, Apr. 2012.

[12] A. J. Stewart and J. B. Plotkin, "From extortion to generosity, evolution in the iterated prisoner's dilemma," *Proc. Nat. Acad. Sci. USA*, vol. 110, no. 38, pp. 15348–15353, Sep. 2013.

[13] C. Adami and A. Hintze, "Evolutionary instability of zero-determinant strategies demonstrates that winning is not everything," *Nat. Commun.*, vol. 4, p. 2193, Aug. 2013.

[14] C. Hilbe, B. Wu, A. Traulsen, and M. A. Nowak, "Cooperation and control in multiplayer social dilemmas," *Proc. Nat. Acad. Sci. USA*, vol. 111, no. 46, pp. 16425–16430, Apr. 2014.

[15] L. Pan, D. Hao, Z. Rong, and T. Zhou, "Zero-determinant strategies in iterated public goods game," *Sci. Rep.*, vol. 5, Feb. 2015, Art. no. 13096.

[16] X. He, H. Dai, P. Ning, and R. Dutta, "Zero-determinant strategies for multi-player multi-action iterated games," *IEEE Signal Process. Lett.*, vol. 23, no. 3, pp. 311–315, Mar. 2016.

[17] H. Q. Zhang, D. Niyato, L. Y. Song, T. Jiang, and Z. Han, "Equilibrium analysis for zero-determinant strategy in resource management of wireless network," in *Proc. IEEE Wireless Commun. Netw. Conf.*, New Orleans, LA, USA, Mar. 2015, pp. 2002–2007.

[18] H. Q. Zhang, D. Niyato, L. Y. Song, T. Jiang, and Z. Han, "Zero-determinant strategy for resource sharing in wireless cooperations," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 2179–2192, Mar. 2016.

[19] A. A. Daoud, G. Kesidis, and J. Liebeherr, "Zero-determinant strategies: A game-theoretic approach for sharing licensed spectrum bands," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 11, pp. 2297–2308, Nov. 2014.

[20] J. Garay, A. Kiayias, and N. Leonardos, "The bitcoin backbone protocol: Analysis and applications," in *Advances in Cryptology—EUROCRYPT*, vol. 9057, E. Oswald and M. Fischlin, Eds. Berlin, Germany: Springer, 2015, pp. 281–310.

[21] B. Johnson, A. Laszka, J. Grossklags, M. Vasek, and T. Moore, "Game-theoretic analysis of DDoS attacks against bitcoin mining pools," in *Proc. Int. Conf. Financ. Cryptography Data Security*, Oct. 2014, pp. 72–86.

[22] C.-B. Tang, Z. Yang, Z.-L. Zheng, Z.-Y. Chen, and X. Li, "Game dilemma analysis and optimization of PoW consensus algorithm," (in Chinese), *Acta Automatica Sinica*, vol. 43, no. 9, pp. 1520–1531, Sep. 2017.

[23] Y. Zhen, M. Yue, C. Zhong-Yu, T. Chang-Bing, and C. Xin, "Zero-determinant strategy for the algorithm optimize of blockchain PoW consensus," in *Proc. 36th Chin. Control Conf.*, Dalian, China, Jul. 2017, pp. 1441–1446.

[24] L. Fan, H. Zheng, J. H. Huang, Z. C. Li, and Y. H. Jiang, "A method of cooperative evolution for blockchain mining pool based on adaptive zero-determinant strategy," (in Chinese), *J. Comput. Appl.*, vol. 39, no. 3, pp. 918–923, 2019.

[25] P. Naghizadeh and M. Y. Liu, "Provision of public goods on networks: On existence, uniqueness, and centralities," *IEEE Trans. Netw. Sci. Eng.*, vol. 5, no. 3, pp. 225–236, Jul./Sep. 2018.

[26] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 2084–2123, 3rd Quart., 2016.

[27] N. Houy, "The bitcoin mining game," *Ledger J.*, vol. 1, no. 13, pp. 53–68, 2016.

[28] F. Garcia, B. Mirbach, B. Ottersten, F. Grandidier, and Á. Cuesta, "Pixel weighted average strategy for depth sensor data fusion," in *Proc. IEEE Int. Conf. Image Process.*, Hong Kong, Sep. 2010, pp. 2805–2808.

[29] J. Liu, Y. Zhang, Y. Zhou, D. Zhang, and H. Liu, "Aggressive resource provisioning for ensuring QoS in virtualized environments," *IEEE Trans. Cloud Comput.*, vol. 3, no. 2, pp. 119–131, Apr./Jun. 2015.

[30] E. A. Abdelaziz, R. Saidur, and S. Mekhilef, "A review on energy saving strategies in industrial sector," *Renew. Sustain. Energy Rev.*, vol. 15, no. 1, pp. 150–168, Jan. 2011.

[31] C. Hilbe, M. A. Nowak, and K. Sigmund, "Evolution of extortion in iterated prisoner's dilemma games," *Proc. Nat. Acad. Sci. USA*, vol. 110, no. 17, pp. 6913–6918, Apr. 2013.