IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 22, 2018, accepted December 17, 2018, date of publication January 2, 2019, date of current version January 23, 2019.

Digital Object Identifier 10.1109/ACCESS.2018.2890391

Pool Strategies Selection in PoW-Based Blockchain Networks: Game-Theoretic Analysis

YUE WANG[1], CHANGBING TANG[1,2], (Member, IEEE), FEILONG LIN[1], (Member, IEEE), ZHONGLONG ZHENG[1], (Member, IEEE), AND ZHONGYU CHEN[1]

[1]College of Mathematics, Physics and Information Engineering, Zhejiang Normal University, Jinhua 321004, China
[2]School of Engineering, RMIT University, Melbourne, VIC 3001, Australia

Corresponding authors: Changbing Tang (tangcb@zjnu.edu.cn) and Zhongyu Chen (czy@zjnu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61503342, Grant 61672467, Grant 61672468, and Grant 61877055, in part by the Zhejiang Provincial Natural Science Foundation of China under Grant LY16F030002 and Grant LY18F030013, and in part by the China Scholarship Council under Grant 201708330402.

ABSTRACT In proof-of-work-based (PoW-based) blockchain networks, the miners participate in a crypto-puzzle solving competition to win the reward by publishing a new block. Open mining pools attract a large number of miners for solving difficult problems together. Although the open strategy is likely to be more efficient, it makes pools susceptible to attack at the same time. In this paper, we present a game-theoretic analysis of mining pool strategy selection in order to explore the trade-off between the efficiency of openness and the vulnerability of attacks in a PoW-based blockchain network. We first model the pool mining process as a two-stage game, wherein the pools might decide whether to open or not and to attack or not. Based on the two-stage game model, we analyze the Nash equilibrium and the evolutionary stability of the mining games among pools, which uncovers the pool selection dynamics of PoW-based blockchain networks. In particular, we find that the attack behavior is the norm for a weak pool and triggers lower expected utilities when punishing the attacks more severely. Numerical simulations also support our theoretical findings as well as demonstrate the stability of the pools' strategy selection.

INDEX TERMS Blockchain, block withholding attack, game theory, Nash equilibrium, evolutionary stability.

I. INTRODUCTION

The blockchain networks are point-to-point (P2P) networks that use a distributed consensus algorithm to generate and update data [1]. More specifically, the blockchain data structure is employed in such networks to verify and store data, the cryptography is utilized to ensure the security of data transmission and access, while the intelligent contracts are adopted to program and manipulate data [2]. As an integrated application of distributed data storage, point-to-point transmission, consensus mechanism, and encryption algorithm, blockchain has recently generated explosive interest from both academia and industry [3]–[7], with many proposed applications, such as big data [8], [9], cloud and edge computing [10], [11], healthcare [12], Internet of things [13], [14], intelligent transportation system [15], electrical energy systems [16], industry security [17], cyber-physical systems [18], social governance [19], and so on. A survey of this topic can be referred to [20] and [21].

As one of the most successful applications of the blockchain technology, the bitcoin system applies the consensus mechanism of proof-of-work (PoW) to realize non-tampered and non-forged transactions [22]. The core idea of the PoW consensus mechanism is to ensure the consistency of data and the security of consensus through the computing power competition of distributed nodes [22]. The nodes compete with each other based on their respective computing power in order to solve a complex SHA256 mathematical problem, which is difficult to solve but easy to verify. The node that solves the problem first accounts for the blocks and obtains the bitcoin rewards generated by the system automatically [23]. In the bitcoin system, the process of producing blocks is called mining, and the participants in the mining are called miners. The system generates one block approximately every 10 *min* on average, which means that a miner with a small fraction of the total mining power is unlikely to be rewarded for a long time [23]. Theoretically, solo miners will take several years to win the block reward, and thus, miners resort to using open pools to increase the possibility of gaining a stable income.

2169-3536 © 2019 IEEE. Translations and content mining are permitted for academic research only.
Personal use is also permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

In open pools, it is easy for participants to register as miners, where participants are only required to provide a public network interface. However, the openness of the pool makes it vulnerable to being attacked [24]. The pool that initiates the attack will infiltrate its partial miners into a victim pool by registering as a regular miner who receives mining tasks from the victim pool [25]. The mining power that the attacker redirects towards the victim's tasks is called the infiltration rate, and the attacking miners are called infiltrating miners [25]. When the attacker receives partial proofs of work (PPoWs) from the infiltrating miners, it sends them to the manager of the victim pool who estimates their true mining power. However, when the attacker receives full proofs of work (FPoWs) from the infiltrating miners, it withholds and discards them. In this case, the victim pool is under the illusion that the infiltrating power is performing effective mining and shares its revenue with the attacking pool. This type of attack is called a block withholding attack [26], [27].

Although pools can increase their profits by attacking other pools, if all miners choose to attack each other, they will gain less profit than if they do not attack each other. This is the mining dilemma in the PoW consensus algorithm, which corresponds to the classic prisoner's dilemma in game theory [28]–[30]. Concretely, attack is the best strategy for a mining pool, but it is not the best strategy for the whole system. Understanding and analyzing the game dilemma in the process of mining undoubtedly provides a theoretical basis for the development and applications of blockchain technology.

At present, several literatures have been focused on the study of the pool game based on game theory. Eyal [25] qualitatively analyzed the Nash equilibrium (NE) of mining game where pools use some of their participants to infiltrate other pools and perform a withholding attack. They also shown the existence conditions of the NE for any number of pools. Liu *et al.* [31] used the evolutionary games to study which pool is chosen on calculating the expected earnings of miners joining different pools. Lewenberg *et al.* [32] transformed the choice of miners to join a mining pool into a cooperative game model, wherein the members of the same pool were regarded as an alliance. They also showed that miners can increase their profits by changing their mining pool. Garay *et al.* [33] used the blockchain bifurcation loophole to map the mining model into a random game with complete information and controlled the length of the main chain through the released time of the succeed mining block. In addition, Kroll *et al.* [34] provided a game theoretic analysis of bitcoin, and argued that the honest strategy constitutes an NE, implying incentive-compatibility. Tang *et al.* [35] analyzed the existence conditions of the NE in the choice of miner strategy during the PoW consensus process and optimized the minerąŕs strategy selection using the zero-determinant strategy. Furthermore, Johnson *et al.* [36] explored the trade-off among DDoS attacks with a series of game-theoretical models of competition between two pools of varying sizes, and found that pools have a greater incentive to attack large pools than small ones.

Motivated by theses references, we apply game theory to explore the selection of pool strategies based on the blockchain network, and study the trade-off between the higher productivity offered by open pools and the increased vulnerability that comes with openness. Generally, mining pools can freely choose an open or closed strategy. Openness might result in a more stable reward but also implies a certain probability of attack. In the actual mining process, pools may decide whether to attack or non-attack and whether to be open or closed. In this paper, we explore the pool selection dynamics of PoW-based blockchain networks through the analysis of the NE and the evolutionary stability, which provides a new idea and method for the security of the blockchain consensus algorithm. The main contributions of this paper are summarized as follows.

- We model the process of mining as a two-layer game model in order to characterize the open-attack decision in the PoW-based blockchain network. Besides, we explore the trade-off between the higher efficiency offered by openness and the increased vulnerability that comes with it in terms of game theory.
- We apply the NE theory for analyzing the effects of the damage caused by the attack and the punishment imposed on the strategy of attack under the condition that both mining pools choose the open strategy. The results show that punishing the attacks more severely does not deter the attackers and triggers lower expected utilities. Besides, with an increase of punishment, the weak pool is inclined to attack other pools.
- In order to overcome the shortcoming that the NE only describe the local optimization of the pool strategies selection, we establish an evolutionary game model for depicting the pool strategies selection under the viewpoint of dynamics. We thus analyze the evolutionary stability of the strategy selection for competitive pools and present the conditions for the stability of the strategy evolution.

The rest of this paper is organized as follows: Section II introduces the NE and evolution stability in the game theory. In Section III, we present the two-layer game model for depicting the open-attack decision in the process of mining. In Section IV, we consider the case wherein both players choose to be open and apply game theory for analyzing the NE and the evolutionary stability of mining pool strategy selection. In Section V, we present a numerical simulation to verify our conclusion. Finally, we summarize the contents of this article in Section VI.

II. PRELIMINARIES

A. NASH EQUILIBRIUM

The NE depicts the best profile of all game players' strategies, i.e., under this profile, all game players' strategies are the best response against their opponents' strategies and no game players will unilaterally change their strategies. From the dynamic viewpoint, the state of the NE actually refers to a fixed point in the strategy profile. At this point, each individual's strategy is a best response to the strategy adopted by all the other individuals.

Let us consider an n-player game with a finite strategy space $A = \prod a_i$, where a_i is the strategy set of the players. Denote $X = (x_1, x_2, \cdots, x_n)$, $x_i \in a_i$, and $x_{-i} = (x_1, \cdots, x_{i-1}, x_{i+1}, \cdots, x_n)$. Let $u_i(X) = u_i(x_i, x_{-i})$ be the player's utility function of strategy x_i corresponding to X.

Definition [37]: An NE $X^* = (x_1^*, x_2^*, \cdots, x_n^*)$ is such a state wherein each individual cannot change his own strategy unilaterally in order to obtain a higher utility, i.e.,

$$u_i\left(x_i^*, x_{-i}^*\right) \geq u_i\left(x_i', x_{-i}^*\right), \quad \forall i,\ x_i^* \in X^*, x_i' \notin X^*. \quad (1)$$

An NE is strict if (1) holds strictly for every $x_i' \neq x_i^*$. If x_i^* is a pure strategy, the equilibrium is a pure NE; otherwise, it is a mixed NE. Every strict NE (SNE) is pure, and thus, we do not use the term strict pure NE but an SNE.

B. EVOLUTIONARY STABILITY

The concept of NE can characterize the outcome of a single static game in which the strategy profile achieves a state such that no player has a unilateral incentive to play another strategy. However, the strategy profile that is beneficial for a given player may not always be beneficial for the entire system. That is to say, NE is only a local optimization concept from the viewpoint of optimization theory. Correspondingly, the concept of an evolutionarily stable strategy (ESS) is proposed in order to depict the dynamical evolution of the whole population.

Assume that the whole population adopts strategy φ, and a small fraction ε (called mutations) adopts strategy ϕ ($\phi \neq \varphi$).

Definition 2 [38]: Evolutionary forces are expected to select φ against ϕ if

$$u(\varphi, \varepsilon\phi + (1-\varepsilon)\varphi) > u(\phi, \varepsilon\phi + (1-\varepsilon)\varphi). \quad (2)$$

Strategy φ is said to be the ESS if for every $\phi \neq \varphi$, and there are some $\hat{\varepsilon}_y > 0$ such that (2) holds for all $\varepsilon \in (0, \hat{\varepsilon}_y)$. That is, φ is an ESS if, after mutation, non-mutants are more successful than mutants. In other words, mutants cannot invade the population and will eventually get extinct [39].

The definition of an ESS is stronger than that of NE, as the former is robust against a deviation of the whole population while the latter is only focused on the deviations of a single player. Although ESS has been originally defined in biological systems, it is highly relevant in the engineering field as well [39]–[42]. Based on the ESS, we can identify robustness against deviations of more than one player. Furthermore, we can apply the convergence theory of evolutionary game dynamics and stability for capturing the effectiveness and robustness of the proposed strategy.

III. SYSTEM MODEL

We study an non-cooperative situation wherein miners compete to solve a crypto-puzzle problem in a PoW-based blockchain network. Assume that there are n miners who are organized into M mining pools in the network. As shown in Fig. 1(a), each pool can choose either closed mining (C) or open mining (O). The open strategy for the mining pool is likely to be more efficient even though the exact level of efficiency is not known, which reflects a high level of uncertainty in network science [43], [44]. The selection of the open strategy implies that every miner, including malicious ones, can join this pool. Further, the openness makes the pool more vulnerable to attacks, which damages the mining efficiency of the whole system. Consequently, in addition to deciding whether to be open or closed, the pools are also required to decide whether to attack others for extra benefits. Thus, each pool can also choose either attack (A) or non-attack (N), as shown in Fig. 1(b).

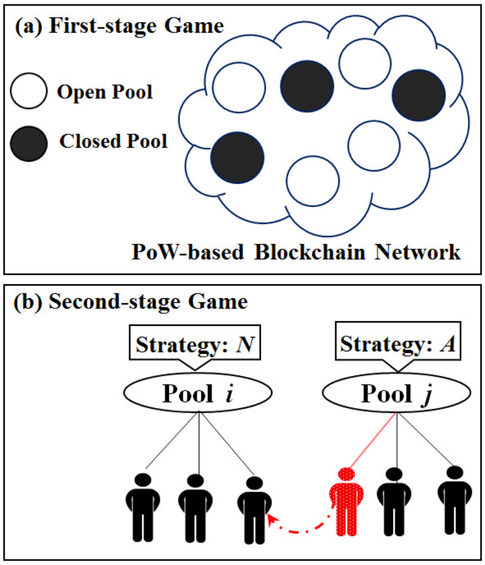

FIGURE 1. **Two-stage game model of the pool strategies selection in a PoW-based blockchain network. (a) First-stage game: each pool can choose either closed mining (*C*) or open mining (*O*); (b) Second-stage game: each pool can choose either attack (*A*) or non-attack (*N*).**

We propose a two-stage game model that isolates these two factors. In this model, a pool decides whether to be open or closed and whether to attack other pools. If the pool chooses to be open, other pools know the global information well and can decide whether to attack. It should be noted that the decisions are sequential, i.e., the decision to be open is made first while the decision about attacking is made second, which causes the interaction to become a sequential two-stage game.

In the first stage, the pools have two strategies to choose from: C and O. Let $P = \{p_1, \cdots, p_i, \cdots, p_M\}$, where p_i represents the mining power of the pool i. The mining power of the closed pool is fixed and is denoted by Q ($Q < min\{p_i\}$). Assume that the open strategy's mining power obeys a uniform distribution between 0 and 1, i.e., $p_i \sim U[0, 1]$. The pool that first solves the crypto-puzzle wins. Assume that the reward for the winning pool is R, and the income of other pools is 0. Without the loss of generality, we normalize $R = 1$ in this work. As the time required for mining the block successfully is inversely proportional to the mining power in the absence of an attack, the higher mining power of the pool results in a greater likelihood of winning the reward. Moreover, as $Q < min\{p_i\}$, the probability of a closed pool mining a block successfully almost tends to 0, where the mining pools cannot attack each other.

In the second stage, the pools decide whether to attack other pools or not, where attack is denoted as A and non-attack is denoted as N. Here, the attacked pool infiltrate miners to other pool and only submit PPoW to the attacked pool as the computational share. Although the attacker does not affect directly the revenue of other pools and does not change the pool's effective mining power, it share the reward from the attacked pool. Therefore, each miner earns less, as the same revenue is distributed among more miners. Let m ($m \in [0, 1]$) be the loss of reward for the attack pool. Here, m can be considered as a punishment for the attack strategy, where the punishment is considered intuitively as an effective mechanism towards the malicious behaviors [45]. In addition, the damage inflicted by the attack is denoted by d ($d \in [0, 1]$), which determines how much mining power is lost because of being attacked. In the following, we characterize the equilibrium of the two-stage game in terms of parameters of m and d.

IV. GAME ANALYSIS OF MINING POOL STRATEGY SELECTION

In this section, we apply game theory for analyzing the equilibrium of the mine pool strategy selection, in which the trade-off between the higher efficiency of openness and the vulnerability of attacks in the blockchain network is investigated. Furthermore, we study the evolutionary stability of the mining games among pools, wherein the dynamics of closed mining and open mining strategies are considered. Since each decision of pool made in the first stage (to be open or closed) results in a different second-stage game (whether to attack or not), we first analyze the second-stage game, based on which, we can analyze how decisions are made in the first-stage.

A. NASH EQUILIBRIUM IN SECOND-STAGE GAME

In this subsection, we consider the interactions between two competitive open mining pools. Without loss of generality, we denote two pools as pool 1 and pool 2, which can be generalized to M pools. Let p_1 and p_2 be the mining power of pool 1 and pool 2, which are known before they decide on attacking. We only consider the case that $p_1 > p_2$, and the other case is symmetric (the case of $p_1 = p_2$ is not effect on the first-stage game). When $p_1 - d > p_2$, the attack by pool 2 does not make its power to exceed the power of pool 1. In this case, the strategy of attack does not change the outcome nor the pool attacks. When $p_1 - d = p_2$, the attack by pool 2 only make its power equal to the power of pool 1. Since the attack will be punished, pool 1 will not choose active attack, and pool 2 only attack when $m < 1/2$. In this case, if pool 1 choose to attack, it will get the utility of $1 - m$, or else, the utility is $1/2 + m$. Further, when $m > 1/4$, pool 1 choose to non-attack. The above two situations have no effect on the first-stage game. Thus, we mainly discuss that $p_1 - d < p_2$, in which a unilateral attack by the weak pool (i.e., pool 2) brings it ahead of the strong pool (i.e., pool 1). Accordingly, when each pool chooses A, the utility of pool 1 is $1 - m$ and that of pool 2 is $-m$; when each pool chooses N, the utility of pool 1 is 1 and that of pool 2 is 0. When pool 1 chooses A and pool 2 chooses N, the utility of the former is $1 - m$, while the utility of the later is m. The payoff matrix of A and N is presented in Table 1.

TABLE 1. **Payoff matrix of the second-stage game.**

	A	N
A	$1-m,-m$	$1-m,m$
N	$m,1-m$	$1,0$

The mining pool game has a unique mixed equilibrium point. Let η_1 and η_2 be the probabilities of pools 1 and 2 attacking, respectively. For pool 1, an attack results in an expected utility of $\eta_2(1 - m) + (1 - \eta_2)(1 - m) = 1 - m$, while an non-attack scenario results in an expected utility of $\eta_2 m + (1 - \eta_2) \cdot 1 = 1 - \eta_2 + \eta_2 m$. In a mixed equilibrium, a pool's expected utility from choosing either actions must be the same, which results in $1 - m = 1 - \eta_2 + \eta_2 m$, i.e.,

$$\eta_2 = \frac{m}{1 - m}. \tag{3}$$

Similarly, for pool 2, the expected utility from an attack is $\eta_1(-m)+(1-\eta_1)(1-m) = 1-m-\eta_1$. The expected utility from an non-attack scenario is $\eta_1 m+(1-\eta_1)\cdot 0 = \eta_1 m$. The mixed equilibrium condition is then satisfied $1 - m - \eta_1 = \eta_1 m$, i.e.,

$$\eta_1 = \frac{1 - m}{1 + m}. \tag{4}$$

Theorem 1: The larger of the value m, the more (less) likely that the weak (strong) pool will attack.

Proof: From Eqs. (3) and (4), it can easily be determined that with an increasing the value of m (increasing the value of punishment), the attacking probability of the strong pool decreases and that of the weak pool increases. Thus, when m increases, the weak pool is inclined to attack, and the strong pool is inclined to refrain from attacking. That is to say, it is norm that a weak pool present an attack behavior when increasing the value of punishment. ■

Remark 1: The behavior in Theorem 1 contradicts the intuition that punishment will prevent the attacks, i.e., the severer punishment of the attack is performed, the lower likelihood of the attacking for strong pool is.

Corollary 1: Increasing the value of m, the weak pool is more likely to win.

Proof: Let p_{win1} and p_{win2} be the probabilities of pool 1 and pool 2 winning the reward, respectively. In the case of

$p_1 - d < p_2$, pool 2 wins when it attacks and pool 1 does not attack, the probability of which is $p_{win2} = \eta_2(1-\eta_1) = \frac{2m^2}{1-m^2}$. Consequently, the probability of pool 1 winning the reward is $p_{win1} = 1 - \frac{2m^2}{1-m^2} = \frac{1-3m^2}{1-m^2}$. The greater the punishment is, the more likely the weak pool is to win. ■

Theorem 2: When the punishment $m > \sqrt{2}-1$, punishing the attacks more severely gives rise to lower expected utilities of the pools.

Proof: Let u_{pool1} and u_{pool2} be the expected utilities of pool 1 and pool 2, respectively. From the above analysis, we know that $u_{pool1} = 1-m$. Thus, increasing the value of m, the utility of pool 1 decreases. On the other hand, the expected utility of pool 2 is

$$u_{pool2} = \eta_1 m = \frac{1-m}{1+m} \cdot m = \frac{m-m^2}{1+m}. \tag{5}$$

Since $u'_{pool2} = \frac{1-2m-m^2}{(1+m)^2}$, then $u'_{pool2} > 0$ when $0 < m < \sqrt{2}-1$, and $u'_{pool2} < 0$ when $m > \sqrt{2}-1$. These means that the utilities of pool 2 decrease with the increasing of m when $m > \sqrt{2}-1$. ■

Remark 2: From Theorem 2, we know that the social welfare of the system decreases when the value of m increases. This result suggests that increasing the punishment of an attack is damaged for the system.

B. EVOLUTIONARY STABILITY IN FIRST-STAGE GAME

In above subsection, we computed the expected utilities in the second-stage game when two competitive pools were open under the condition $p_1 - d < p_2$, in which we can see the influence of parameters m and d on the attack strategy and the profit of the mining pool. We now take a step back and compute the expected utilities when two competitive pools are open but before their mining power has become known.

(i) When both pools use an open strategy O, the utility of pool 1 (and symmetrically, that of pool 2) is

$$\begin{aligned}\mathbf{U} &= P(p_2 < p_1 < p_2+d)(1-km) + P(p_2+d < p_1)\cdot 1\\ &\quad + P(p_1 < p_2 - d)\cdot 0 + P(p_2 - d < p_1 < p_2)\left(\frac{m-m^2}{1+m}\right)\\ &= P(p_2 < p_1 < p_2+d)(1-m) + P(p_2+d < p_1)\\ &\quad + P(p_2 - d < p_1 < p_2)\left(\frac{m-m^2}{1+m}\right). \end{aligned} \tag{6}$$

The first term corresponds to the utility of pool 1 in the mixed equilibrium of the game under the condition $p_2 < p_1 < p_2 + d$. The second term corresponds to the utility of pool 1 when pool 2 cannot overtake pool 1 even after attacking it under the condition $p_2 + d < p_1$. The third term corresponds to the utility of pool 1 when pool 1 cannot reach pool 2 even after attacking ($p_1 < p_2 - d$), and the forth term corresponds to the utility of pool 1 in the mixed equilibrium of the game under the condition ($p_2 - d < p_1 < p_2$). Under the assumption that p_i is uniformly distributed between 0 and 1, we have

$$\begin{aligned} P(p_2+d < p_1) &= \int_0^1 \int_0^1 1_{(p_2+d<p_1)} dp_2 dp_1\\ &= \int_d^1 \int_0^{p_1-d} 1 dp_2 dp_1\\ &= \frac{1}{2} - d + \frac{d^2}{2}, \end{aligned} \tag{7}$$

$$\begin{aligned} P(p_2 < p_1 < p_2+d) &= \int_0^1 \int_0^1 1_{(p_2<p_1<p_2+d)} dp_2 dp_1\\ &= \int_0^1 \int_{p_2}^{min\{p_2+d,1\}} 1 dp_2 dp_1\\ &= \int_0^1 (min\{p_2+d, 1\} - p_2) dp_2 dp_1\\ &= \int_0^{1-d} d\cdot dp_2 + \int_{1-d}^1 (1-p_2) dp_2\\ &= d - \frac{d^2}{2}, \end{aligned} \tag{8}$$

$$\begin{aligned} P(p_2 - d < p_1 < p_2) &= \int_0^1 \int_0^1 1_{p_2-d<p_1<p_2} dp_2 dp_1\\ &= \int_0^1 \int_{max\{p_2-d,0\}}^{p_2} 1 dp_2 dp_1\\ &= \int_0^1 (p_2 - max\{p_2-d, 1\}) dp_2 dp_1\\ &= \int_0^d p_2 dp_2 + \int_d^1 d\cdot dp_2 = d - \frac{d^2}{2}. \end{aligned} \tag{9}$$

The utility of each pool is

$$\begin{aligned} \mathbf{U} &= (d - \frac{d^2}{2})(1-m) + (\frac{1}{2} - d + \frac{d^2}{2})\cdot 1\\ &\quad + (d - \frac{d^2}{2})(\frac{m-m^2}{1+m})\\ &= \frac{1}{2} - m(d - \frac{d^2}{2}) + (d - \frac{d^2}{2})(\frac{m-m^2}{1+m})\\ &= \frac{1}{2} - (d - \frac{d^2}{2})(\frac{2m^2}{1+m}). \end{aligned} \tag{10}$$

The utility of each pool decreases as both m and d increase. In the extreme case, when both m and d are 1, the utility is 0. Whenever either of the parameters is at its minimum value of 0, the utility is at its maximum value of $1/2$.

(ii) When both pools use a closed strategy C, there is no reason to attack, and they both choose N in the second stage. Each pool is equally likely to win, and the expected utility of each pool is $1/2$.

(iii) When pool 1 is open and pool 2 is closed, pool 1 cannot attack but pool 2 attacks if doing so causes it to overtake pool 1. Pool 2 attacks if the realized mining power of pool 1 is less than the damage, i.e., $p_1 < d$, then pool 2 can win. As the power of the open strategy is higher than that of the closed strategy, the utility of pool 1 is

$$d\cdot(0+m) + (1-d)\cdot 1 = 1 - d + md. \tag{11}$$

From Eq. (11), we know that pool 1 receives a payoff of 1 when its mining power is sufficiently high in order to remain free from attack, the probability of which is $1-d$. Furthermore, pool 1 receives a payoff of m when its mining power is sufficiently low for it to be overtaken, probability of which is d. Similarly, the utility of pool 2 is

$$(1-d)\cdot 0 + d(1-m) = d(1-m). \tag{12}$$

Thus, the mining power of pool 1 is sufficiently low for it to be overtaken after an attack (which has a probability of d), and thus, pool 2 attacks and receives the reward minus the punishment, i.e., $1-m$. For pool 2, attacking pool 1 results in a positive utility while not attacking pool 1 results in a zero utility. The case in which pool 2 is open and pool 1 is closed is symmetrical. From the above analysis, we obtain the payoff matrix shown in Table 2.

TABLE 2. **Payoff matrix of the first-stage game.**

	O	C
O	$\frac{1}{2}-(d-\frac{d^2}{2})\cdot\frac{2m^2}{1+m}, \frac{1}{2}-(d-\frac{d^2}{2})\cdot\frac{2m^2}{1+m}$	$1-d+md, d(1-m)$
C	$d(1-m), 1-d+md$	$\frac{1}{2}, \frac{1}{2}$

Based on the payoff matrix of first-stage game in Table 2, we can apply evolutionary game theory to explore the evolutionary stability of mining pool's open strategy selection. Consider a system with M pools to mine the blocks together. In each mining operation, each pool randomly selects another pool to form a game pair. For each mining pool, they exist two strategies: O and C. Denote x_1 and x_2 as the frequencies of the strategies O and C, respectively. Thus, $x_1+x_2=1$. We can obtain the expected utility of each strategy from the payoff matrix, as shown in Table 2. For a game player adopting strategy O, the probabilities of him meeting the opponents of strategy O and C are x_1 and x_2, respectively. Thus, the expected payoff of the pools on when they adopting strategies O and C are as follows

$$\begin{cases} P_1 = x_1[\frac{1}{2}-(d-\frac{d^2}{2})\cdot\frac{2m^2}{1+m}] + x_2(1-d+md) \\ P_2 = x_1[d(1-m)] + \frac{1}{2}x_2. \end{cases} \tag{13}$$

According to the pairwise proportional imitation protocol [38], we can use the replicator dynamic equation to approximate the evolution dynamics of the population

$$\dot{x}_i(t) = x_i(P_i-\bar{P}), \quad i=1,2, \tag{14}$$

where $\bar{P}=\sum_{i=1}^{2} x_iP_i$ represents the average payoff of the strategy. We can then obtain the following frequency change rate equation of each strategy

$$\begin{cases} \dot{x_1}(t) & = x_1(P_1-\bar{P}) \\ & = [\frac{1}{2}-(d-\frac{d^2}{2})\cdot\frac{2m^2}{1+m}](x_1^2-x_1^3) \\ & +(x_1x_2-x_1^2x_2)(1-d+md) \\ & -x_1^2x_2[d(1-m)] - \frac{1}{2}x_1x_2^2 \\ \dot{x_2}(t) & = x_2(P_2-\bar{P}) \\ & = \frac{1}{2}(x_2^2-x_2^3) + (x_1x_2-x_2^2x_1)d(1-m) \\ & -x_1^2x_2[\frac{1}{2}-(d-\frac{d^2}{2})\cdot\frac{2m^2}{1+m}] \\ & -x_1x_2^2(1-d+md) \end{cases} \tag{15}$$

Let $\dot{x_i}(t)=0$, $(i=1,2)$, then we can obtain two rest points of the Eq. (15) in the form of $(1,0)$ and $(0,1)$. Here, the states $(1,0)$ and $(0,1)$ indicate that all the pools adopt strategies O and C, respectively. We are now ready to investigate the evolutionary stability of these two fixed points. In practical scenarios, the blockchain network is composed of a large population of miners. We can thus apply an asymptotic analysis and obtain the following theorem on the evolutionary stability of the rest points.

Theorem 3: (*i*) The state of $(1,0)$ is an *ESS* if

$$d(1-m)+(d-\frac{d^2}{2})\cdot\frac{2m^2}{1+m} < \frac{1}{2}; \tag{16}$$

(*ii*) The state of $(0,1)$ is an *ESS* if $m < 1-\frac{1}{2d}$.

Proof: For the equilibrium point: $x_1=x^*, x_2=1-x^*, (x^*\in\{0,1\})$, the Jacobi matrix at this point is

$$J = \begin{bmatrix} J_{11} & J_{12} \\ J_{21} & J_{22} \end{bmatrix} = \begin{bmatrix} \frac{\partial f_1(x)}{\partial x_1} & \frac{\partial f_1(x)}{\partial x_2} \\ \frac{\partial f_2(x)}{\partial x_1} & \frac{\partial f_2(x)}{\partial x_2} \end{bmatrix}_{x_1=x^*, x_2=1-x^*} \tag{17}$$

Furthermore, the elements are derived as follows

$$\begin{cases} \frac{\partial f_1(x)}{\partial x_1} = [\frac{1}{2}-(d-\frac{d^2}{2})\cdot\frac{2m^2}{1+m}](2x_1-3x_1^2) \\ \quad + (x_2-2x_1x_2)(1-d+md) \\ \quad - 2x_1x_2[d(1-m)] - \frac{1}{2}x_2^2 \\ \frac{\partial f_1(x)}{\partial x_2} = (x_1-x_1^2)(1-d+md) - x_1^2d(1-m) \\ \quad - x_1x_2 \\ \frac{\partial f_2(x)}{\partial x_1} = (x_2-x_2^2)d(1-m) - x_2^2(1-d+md) \\ \quad - 2x_1x_2[\frac{1}{2}-(d-\frac{d^2}{2})\cdot\frac{2m^2}{1+m}] \\ \frac{\partial f_2(x)}{\partial x_2} = \frac{1}{2}(2x_2-3x_2^2) - x_1^2[\frac{1}{2}-(d-\frac{d^2}{2})\cdot\frac{2m^2}{1+m}] \\ \quad + (x_1-2x_2x_1)d(1-m) - 2x_1x_2(1-d+md). \end{cases} \tag{18}$$

When $x^*=1$, the corresponding Jacobi matrix is

$$J|_{x_1=1,x_2=0} = \begin{bmatrix} J_{11} & J_{12} \\ J_{21} & J_{22} \end{bmatrix},$$

where $J_{11} = -\frac{1}{2}+(d-\frac{d^2}{2})\cdot\frac{2m^2}{1+m}$, $J_{12} = -d(1-m)$, $J_{21} = 0$, and $J_{22} = d(1-m)-\frac{1}{2}+(d-\frac{d^2}{2})\cdot\frac{2m^2}{1+m}$. Its corresponding eigenvalue is

$$\begin{cases} \lambda_1 = -\dfrac{1}{2}+(d-\dfrac{d^2}{2})(\dfrac{2m^2}{1+m}) \\ \lambda_2 = d(1-m)-\dfrac{1}{2}+(d-\dfrac{d^2}{2})\cdot\dfrac{2m^2}{1+m}. \end{cases} \tag{19}$$

When $(d-\frac{d^2}{2})\cdot\frac{2m^2}{1+m} < \frac{1}{2}$, $\lambda_1 < 0$; and when $d(1-m)+(d-\frac{d^2}{2})\cdot\frac{2m^2}{1+m} < \frac{1}{2}$, $\lambda_2 < 0$. Thus, state $(1, 0)$ is stable.

When $x^* = 0$, the corresponding Jacobi matrix is

$$J\,|_{x_1=0,x_2=1} = \begin{bmatrix} \frac{1}{2}-d+md & 0 \\ 1-d+md & -\frac{1}{2} \end{bmatrix}.$$

Its corresponding eigenvalue is

$$\begin{cases} \lambda_1 = -\dfrac{1}{2} \\ \lambda_2 = \dfrac{1}{2}+md-d. \end{cases} \tag{20}$$

When $m < 1-\frac{1}{2d}$, $\lambda_2 < 0$, and thus, state $(0, 1)$ is stable. ■

V. NUMERICAL SIMULATIONS

In this section, we present the numerical analysis used for verifying the above conclusions. Consider a network with $n = 5000$ individual miners which evolves to form 500 mining pools (i.e., $M = 500$).

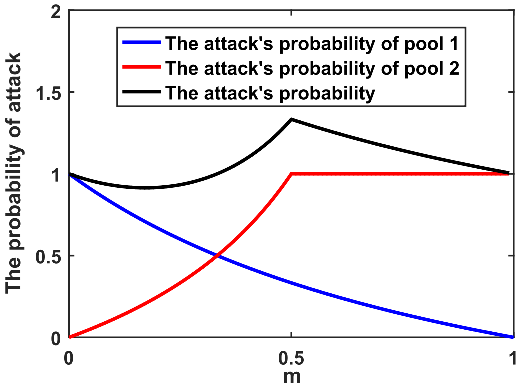

FIGURE 2. **The attacked probability of pools with increasing *m* when $p_2 < p_1 < p_2 + d$.**

In order to investigate the trade-off between the higher efficiency of openness and vulnerability to attacks, we first consider the effects of the parameters m and d on the strategy of attack. Fig. 2 shows that in mining games, increasing the value of m has a small effect on the total number of attacks, i.e., the increasing value of m does not help in preventing attack behavior. Moreover, in the case that both mining pools are open and $p_2 < p_1 < p_2 + d$, the probability of pool 1 choosing to attack decreases from 1 to 0 with the increasing of m from 0 to 1. In contrast, the probability of pool 2 choosing to attack increases as m increases and reaches a maximum value of 1 at $m = 0.5$. Furthermore, the total number of attacks also reaches a maximum at $m = 0.5$.

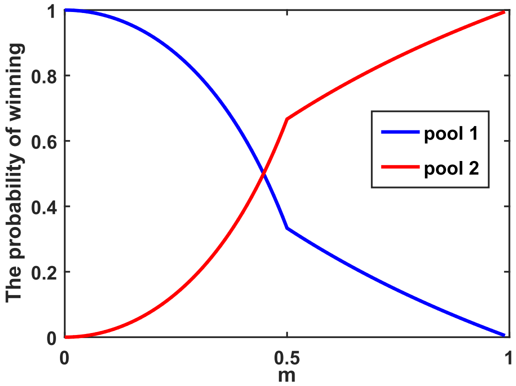

FIGURE 3. **The mining probability of pools with increasing *m* when $p_2 < p_1 < p_2 + d$.**

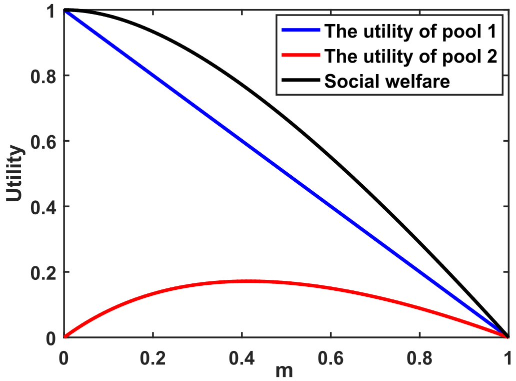

FIGURE 4. **The utilities of pools obtained with increasing *m* when both pools are open and $p_2 < p_1 < p_2 + d$.**

In Fig. 3, we illustrate the variation of the pools' winning probability with the increase in m when both pools are open and $p_2 < p_1 < p_2 + d$. It is shown that the probability of the strong pool winning gradually decreases as the punishment for attacking increases, while the probability of the weak pool winning gradually increases as the punishment for attacking increases. This does not contribute to the entire system's welfare. From the viewpoint of optimization, it is beneficial to set the punishment to 0, because the probability of the strong pool winning is 1 at this time. It is shown in Fig. 4 that the utility of strong pool decreases when the punishment m increases under the conditions that the two pools are both open and $p_2 < p_1 < p_2 + d$. Moreover, the utility of the weak pool first increases and then decreases as m increases under the same conditions. In addition, a higher punishment m is not beneficial to the social welfare of the entire system. Figure 5 shows that when the two pools are open, the increase in m and d results in a lower social welfare. This provides a certain reference for the design of the mining incentive model, i.e., increasing the value of m and d does not contribute to the overall optimization.

Later, we demonstrate the evolutionary stability of the mining games among 500 pools. Set $d = 0.2$ and $m = 0.2$ such

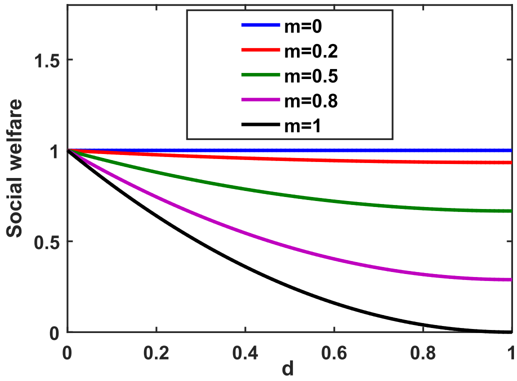

FIGURE 5. The social welfare of the system obtained vs the increasing of d under different values of m.

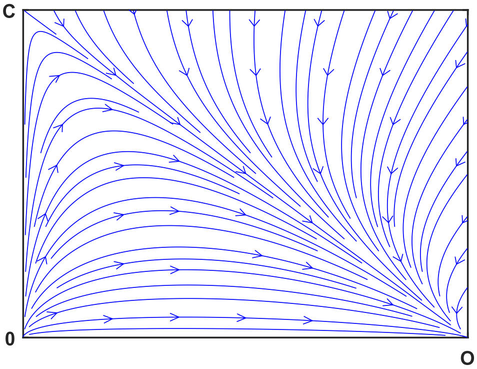

FIGURE 6. Replicator dynamics of the pool selection strategies and the evolution trajectory from $x(0) = (0.25, 0.75)$ with $d = 0.2$ and $m = 0.2$.

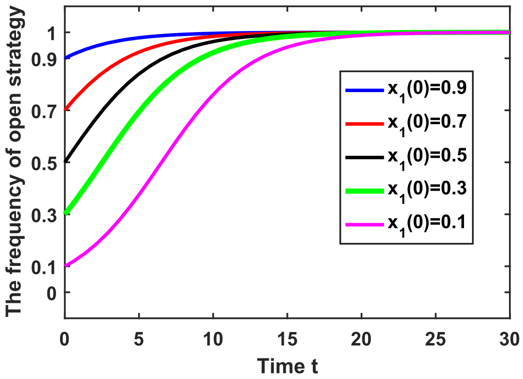

FIGURE 7. Evolution of the pool's population states over time with $d = 0.2$ and $m = 0.2$ for various initializations.

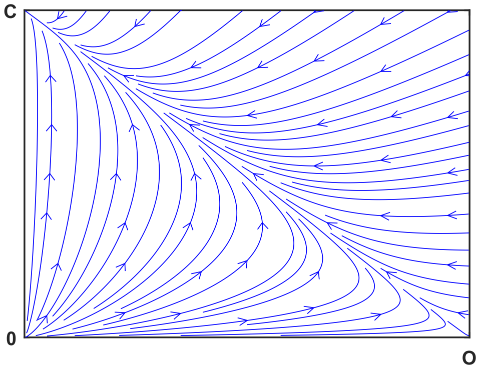

FIGURE 8. Replicator dynamics of the pool selection strategies and the evolution trajectory from $x(0) = (0.25, 0.75)$ with $d = 0.8$ and $m = 0.2$.

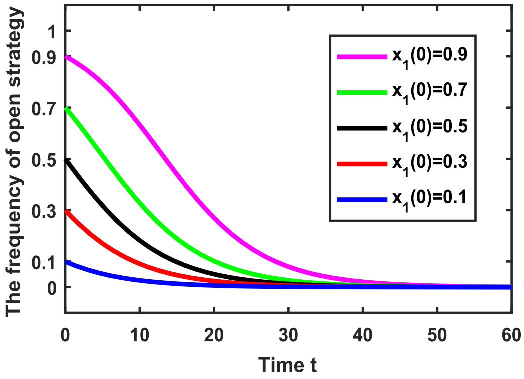

FIGURE 9. Evolution of the pool's population states over time with $d = 0.8$ and $m = 0.2$ for various initializations.

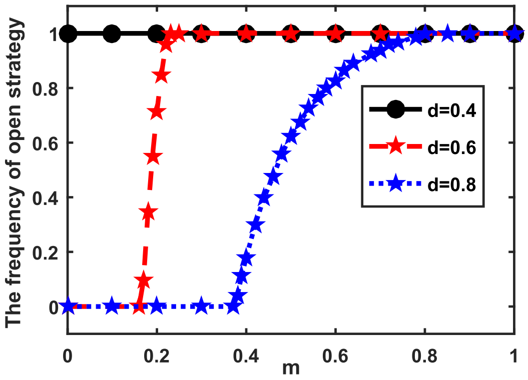

FIGURE 10. The frequency of strategy O as m varies for various values of d.

that the condition (i) in Theorem 3 is satisfied. It is shown in Fig. 6 that strategy C is evolutionarily stable with an initial point $x(0) = (0.25, 0.75)$. Fig. 7 shows that the stable state $x^* = (1, 0)$ is independent of the initializations. Therefore, the pool selection game admits a unique ESS of $x^* = (1, 0)$ and the mining pool tends to choose strategy O, which is in accordance with our theoretical finding (i) in Theory 3. In contrast, we set $d = 0.8$ and $m = 0.2$, which satisfy the condition (ii) in Theorem 3, and there is a unique ESS of $x^* = (0, 1)$. Fig. 8 shows that strategy C is evolutionarily stable with an initial point $x(0) = (0.25, 0.75)$. Fig. 9 demonstrates that there is a unique ESS of $x^* = (0, 1)$, and the mining pool tends to choose strategy C, which is independent of the initializations.

Finally, we examine the evolution of the stable states with respect to various values of m and d for the same network settings. As shown in Fig. 10, increasing the value of m is beneficial for the appearance of the all O stable state. Furthermore, there exists a critical value of m that leads to the stable of state transforming from all C to all O. Moreover, the

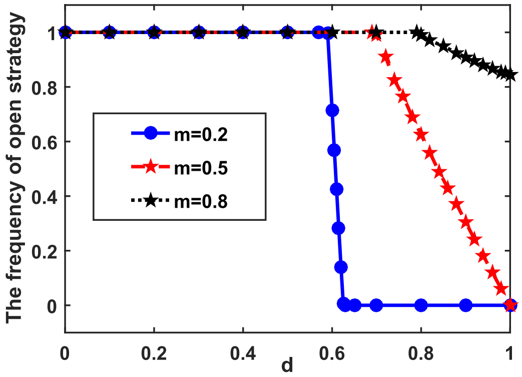

FIGURE 11. The frequency of strategy *O* as *d* varies for various values of *m*.

larger the value of d, the greater critical value of d is. And thus, decreasing the value of d promotes the appearance of the all O stable state. When $d = 0.4$, the frequency of strategy O is maintained at a value of 1 regardless of the value of m. Similarly, it is shown in Fig. 11 that increasing the value of d inhibits the appearance of the strategy O's stable state. There is also a critical value of d that gives rise to the stable of state transforming from all O to all C.

VI. CONCLUSIONS

In this paper, we have treated the damage caused by the attack and the punishment which affect the choice of the mining pool's strategy. We have modeled the mining pool selection as a two-stage game, where there is only one winner in the competition. Based on the game theory, we have analyzed the NE of the two-stage game and found that malicious behavior is the expected behavior. Furthermore, we have investigated the evolutionary stability of the pool selection dynamics for competitive pools and revealed the conditions for the network to admit a unique evolutionary stable state. The numerical evaluation results in this study have provided the evidence for our theoretical discoveries.

Our results emphasize that despite open mining being a more efficient method of mining blocks, it is also a less secure approach. In such distributed and competitive scenarios, it is natural for a selfish player to hurt its opponents, and thus, attacks on other players are essentially unavoidable. We expect the results obtained in this work to hold in a variety of more complicated scenarios that exhibit a fundamental trade-off among efficiency, openness and vulnerability. Furthermore, we expect our work provides a new idea and method for the security of the blockchain consensus algorithm.

REFERENCES

[1] 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.

[2] T. McConaghy *et al.* (2016). *BigchainDB: A Scalable Blockchain Database*. [Online]. Available: https://www.bigchaindb.com/whitepaper/bigchaindb-whitepaper.pdf

[3] Y. Yuan and F.-Y. Wang, "Blockchain: The state of the art and future trends," (in Chinese), *Acta Autom. Sinica*, vol. 42, no. 4, pp. 481–494, Apr. 2016.

[4] P. K. Sharma, S. Singh, Y. S. Jeong, and J. H. Park, "DistBlockNet: A distributed blockchains-based secure SDN architecture for IoT networks," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 78–85, Sep. 2017.

[5] 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.

[6] Y. H. Zhang, R. H. Deng, J. Shu, K. Yang, and D. Zheng, "TKSE: Trustworthy keyword search over encrypted data with two-side verifiability via blockchain," *IEEE Access*, vol. 6, pp. 31077–31087, Jun. 2018.

[7] C. Xu, K. Wang, and M. Guo, "Intelligent resource management in blockchain-based cloud datacenters," *IEEE Cloud Comput.*, vol. 4, no. 6, pp. 50–59, Nov. 2017.

[8] E. Karafiloski and A. Mishev, "Blockchain solutions for big data challenges: A literature review," in *Proc. IEEE 17th Int. Conf. Smart Technol. (EUROCON)*, Ohrid, Republic of Macedonia, Jul. 2017, pp. 763–768.

[9] T. D. Smith, "The blockchain litmus test," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Boston, MA, USA, Dec. 2017 pp. 2299–2308.

[10] Y. Zhang, R. H. Deng, X. Liu, and D. Zheng, "Blockchain based efficient and robust fair payment for outsourcing services in cloud computing," *Inf. Sci.*, vol. 462, pp. 262–277, Jun. 2018.

[11] Z. Xiong, S. Feng, W. Wang, D. Niyato, P. Wang, and Z. Han, "Cloud/Fog computing resource management and pricing for blockchain networks," *IEEE Internet Things J.*, to be published, doi: 10.1109/JIOT.2018.2871706.

[12] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control," *J. Med. Syst.*, vol. 40, no. 10, p. 218, Oct. 2016.

[13] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, May 2016.

[14] L. Zhou, L. Wang, Y. Sun, and P. Lv, "BeeKeeper: A blockchain-based iot system with secure storage and homomorphic computation," *IEEE Access*, vol. 6, pp. 43472–43488, Jun. 2018.

[15] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1832–1843, Dec. 2017.

[16] J. Zhang *et al.*, "Blockchain based intelligent distributed electrical energy systems: needs, concepts, approaches and vision," (in Chinese), *Acta Autom. Sinica*, vol. 43, no. 9, pp. 1544–1554, Sep. 2017.

[17] A. Bahga and V. K. Madisetti, "Blockchain platform for industrial Internet of Things," *J. Softw. Eng. Appl.*, vol. 9, no. 10, p. 533, 2016.

[18] Y. Zhao, Y. Li, Q. Mu, B, Yang, and Y. Yu, "Secure pub-sub: Blockchain-based fair payment with reputation for reliable cyber physical systems," *IEEE Access*, vol. 6, pp. 12295–12303, Jan. 2018.

[19] M. Sharples and J. Domingue, "The blockchain and kudos: A distributed system for educational record, reputation and reward," in *Proc. Eur. Conf. Technol. Enhanced Learn.*, Lyon, France, Sep. 2016, pp. 490–496.

[20] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congr.)*, Honolulu, HI, USA, Jun. 2017, pp. 557–564.

[21] W. Gao, W. G. Hatcher, and W. Yu, "A survey of blockchain: Techniques, applications, and challenges," in *Proc. 27th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Hangzhou, China, Jul./Aug. 2018, pp. 1–11.

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

[23] 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. Secur.*, Dallas, TX, USA, Oct./Nov. 2017, pp. 195–209.

[24] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," *Commun. ACM*, vol. 61, no. 7, pp. 95–102, Jul. 2018.

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

[26] S. Bag, S. Ruj, and K. Sakurai, "Bitcoin block withholding attack: Analysis and mitigation," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 8, pp. 1967–1978, Aug. 2017.

[27] D. K. Tosh, S. Shetty, X. Liang, C. A. Kamhoua, K. A. Kwiat, and L. Njilla, "Security implications of blockchain cloud with analysis of block withholding attack," in *Proc. 17th IEEE/ACM Int. Symp. Cluster, Cloud Grid Comput.*, Madrid, Spain, May 2017, pp. 458–467.

[28] K. Sigmund, *The Calculus of Selfishness*. Princeton, U.K.: Princeton Univ. Press, 2010.

[29] Z. H. Rong, Z.-X. Wu, D. Hao, M. Z. Q. Chen, and T. Zhou, "Diversity of timescale promotes the maintenance of extortioners in a spatial prisoner's dilemma game," *New J. Phys.*, vol. 17, no. 3, p. 033032, 2015.

[30] C.-Y. Xia, S. Meloni, M. Perc, and Y. Moreno, "Dynamic instability of cooperation due to diverse activity patterns in evolutionary social dilemmas," *Europhys. Lett.*, vol. 109, no. 5, p. 58002, 2015.

[31] X. Liu, W. 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.

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

[33] J. Garay, A. Kiayias, and N. Leonardos, "The bitcoin backbone protocol: Analysis and applications," in *Advances in Cryptology-EUROCRYPT*. Berlin, Germany: Springer, Apr. 2015, pp. 281–310.

[34] J. A. Kroll, I. C. Davey, and E. W. Felten, "The economics of bitcoin mining, or bitcoin in the presence of adversaries," in *Proc. Workshop Econ. Inf. Secur.*, 2013, pp. 1–21.

[35] 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 Autom. Sinica*, vol. 43, no. 9, pp. 1520–1531, Sep. 2017.

[36] 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. Financial Cryptogr. Data Secur.*, Oct. 2014, pp. 72–86.

[37] J. F. Nash, Jr., "Equilibrium points in n-person games," *Proc. Nat. Acad. Sci. USA*, vol. 36, no. 1, pp. 48–49, Jan. 1950.

[38] J. Hofbauer and K. Sigmund, *Evolutionary Games and Population Dynamics*. Cambridge, U.K.: Cambridge Univ. Press, 1998.

[39] H. Tembine, E. Altman, R. El-Azouzi, and Y. Hayel, "Evolutionary games in wireless networks," *IEEE Trans. Syst., Man, Cybern. B, Cybern.*, vol. 40, no. 3, pp. 634–646, Jun. 2010.

[40] C. Tang, A. Li, and X. Li, "When reputation enforces evolutionary cooperation in unreliable MANETs," *IEEE Trans. Cybern.*, vol. 45, no. 10, pp. 2190–2201, Oct. 2015.

[41] P. Semasinghe, E. Hossain, and K. Zhu, "An evolutionary game for distributed resource allocation in self-organizing small cells," *IEEE Trans. Mobile Comput.*, vol. 14, no. 2, pp. 274–287, Feb. 2015.

[42] X. Y. Deng, D. Q. Han, J. Dezert, Y. Deng, and Y. Shyr, "Evidence combination from an evolutionary game theory perspective," *IEEE Trans. Cybern.*, vol. 46, no. 9, pp. 2070–2082, Sep. 2016.

[43] B. Golub and M. O. Jackson, "Using selection bias to explain the observed structure of Internet diffusions," *Proc. Nat. Acad. Sci. USA*, vol. 107, no. 24, pp. 10833–10836, 2010.

[44] J. L. Iribarren and E. Moro, "Impact of human activity patterns on the dynamics of information diffusion," *Phys. Rev. Lett.*, vol. 103, no. 3, p. 038702, 2009.

[45] J. M. Galea, E. Mallia, J. Rothwell, and J. Diedrichsen, "The dissociable effects of punishment and reward on motor learning," *Nature Neurosci.*, vol. 18, pp. 597–602, Apr. 2015.

YUE WANG is currently a Junior Student with the Department of Communication Engineering, Zhejiang Normal University, Jinhua, China. Her research interests include game theory and its application in blockchain.

CHANGBING TANG (M'16) received the B.S. and M.S. degrees in mathematics and applied mathematics from Zhejiang Normal University, Jinhua, China, in 2004 and 2007, respectively, and the Ph.D. degree from the Department of Electronic Engineering, Fudan University, Shanghai, in 2014. He is currently an Associate Professor with the Department of Electronics Information and Engineering, Zhejiang Normal University. His research interests include complex networks, game theory and application, blockchain, and optimal control. He was a recipient of the Academic New Artist Doctoral Post Graduate Award from the Ministry of Education of China, in 2012.

FEILONG LIN (M'16) received the B.S. and M.S. degrees in electronic and information engineering from Xidian University, Xi'an, China, in 2004 and 2007, respectively, and the Ph.D. degree from the Department of Automation, Shanghai Jiao Tong University, in 2016. He is currently a Lecturer with the Department of Computer Science and Engineering, Zhejiang Normal University, Jinhua, China. His research interests include the industrial Internet of Things, blockchain, and its applications.

ZHONGLONG ZHENG (M'16) received the B.S degree in electronic engineering from the China University of Petroleum, in 1999, and the Ph.D. degree from the Department of Automation, Shanghai Jiao Tong University, in 2005. He is currently a Full Professor with the Department of Computer Science and Engineering, Zhejiang Normal University, Jinhua, China. His research interests include machine learning, data mining, and blockchain.

ZHONGYU CHEN received the Ph.D. degree from the College of Computer, Shanghai University, in 2011. He is currently a Full Professor with the Department of Computer Science and Engineering, Zhejiang Normal University, Jinhua, China. His research interests include formal methods, requirement modeling, and blockchain applications.