IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 11, 2019, accepted September 28, 2019, date of publication October 4, 2019,
date of current version October 16, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2945600

Mining Pool Manipulation in Blockchain Network Over Evolutionary Block Withholding Attack

SEONGGEUN KIM, (Student Member, IEEE), AND SANG-GEUN HAHN, (Member, IEEE)
Department of Mathematical Sciences, Korea Advanced Institute of Science and Technology, Daejeon 34141, South Korea

Corresponding author: Seonggeun Kim (sunken@kaist.ac.kr)

This work was supported by the Information and Communication Technology Promotion (IITP) Grant Funded by the Korean Government (MSIT) (The mathematical structure of functional encryption and its analysis) under Grant 2016-6-00598.

ABSTRACT In the current blockchain network, many participants rationally migrate the pool to receive a better compensation according to their contribution in situations where the pools they engage encounter undesirable attacks. The Nash equilibria of attacked pool has been widely analyzed, but the analysis of practical methodology for obtaining it is still inadequate. In this paper, we propose an evolutionary game theoretic analysis of Proof-of-Work (PoW) based blockchain network in order to investigate the mining pool dynamics affected by malicious infiltrators and the feasibility of autonomous migration among individual miners. We formulate a revenue model for mining pools which are implicitly allowed to launch a block withholding attack. Under our mining game, we analyze the evolutionary stability of Nash equilibrium with replicator dynamics, which can explain the population change with time between participated pools. Further, we explore the statistical approximation of successful mining events to show the necessity of artificial manipulation for migrating. Finally, we construct a better response learning based on the required block size which can lead to our evolutionarily stable strategy (ESS) with numerical results that support our theoretical discoveries.

INDEX TERMS Blockchain, block withholding attack, evolutionary game theory, mining pool selection, proof-of-work, replicator dynamics.

I. INTRODUCTION

After Satoshi Nakamoto first proposed the Bitcoin in 2008 [1], the blockchain network has attracted tremendous attentions from both industry and academia as a breakthrough technology. The blockchain network is a global ledger maintained by a public and credible decentralized system, which contains the full history of all the transactions ever processed. Due to its innovative potential benefits in terms of cost-efficiency, security and reliability from no intermediary, blockchain has recently explored into a broad range of fields such as smart contracts [2]–[4], Internet of Things (IoT) [5]–[10], big data [11], smart grid [12]–[15], edge computing [16]–[18], medical purpose [19], [20], etc.

In order to prevent the alteration from malicious participants, blockchain applies several types of consensus algorithm which can maintain the integrity of whole network. The Nakamoto protocol, a core consensus algorithm used in Bitcoin, adopts a crypto-puzzle solving process which is implemented by a Proof-of-Work (PoW) mechanism [1]. PoW requires miners to exert significant computing power by exhaustively querying a SHA-256 hash function, and the first miner who proved their work is allowed to generate a valid block in blockchain network. To increase their successful mining rate, they have tried various strategies. In particular, the average time of each mining step is intended to be constant while steadily increases the difficulty of mining. Even though the expected revenue of solo miners is positive, they have to wait for such time interval to generate a consecutive block. Therefore, miners have organized mining pools which engage in sharing both mining reward and workload to reduce the risk [21].

Typical mining pools consist of pool manager and individual miners. The differentiated role of pool manager is outsourcing the work to miners and conducting the blockchain protocol. Miners are required to submit partial proof-of-work (PPoW) and full proof-of-work (FPoW), and if a miner solves and submits a FPoW then pool manager propagates that block to the whole blockchain system. After receiving a reward for generating a valid block, the pool manager distributes it to

The associate editor coordinating the review of this manuscript and approving it for publication was Bilal Alatas.

own miners depending on their relative contributions based on the fraction of submitted solutions including PPoWs. That is, to the bad side, an individual miner can earn a profit without full exertion for solving FPoW unless they are caught on neglect of duty.

Due to the above weakness of PoW consensus, such mining pools are susceptible to several classical attacks on blockchain [21]–[23]. In a block withholding attack, a miner submits only PPoWs and discards FPoWs in order to exploit the shared revenue while reducing the relative mining effort with respect to honest miners [22]. Especially, Slushpool has about 240,000 miners carrying on Bitcoin as of August 2019 whose network hash rate is about 12%. If we assume all pools have a similar aspect in numbers of miners, there are likely to be over a million individuals mining bitcoins. Since only 144 blocks per day are mined on average in bitcoin and the fork rate due to the propagation delay has decreased substantially in the past years [24], even if an individual miner cannot submit a single FPoW for one year, there is nothing unnatural. Although this scenario is now widely known, many pools based on PoW consensus is still vulnerable to block withholding attack since no concrete and effective solution is emerged yet.

Motivated by the above arguments, Eyal first applied a game modelling between two mining pools where both intentionally launch a block withholding attack each other [25], which is built upon one of the key observations of present research [21]. The remarkable study of Eyal is called a *miner's dilemma*: the Nash equilibrium can be obtained by attacking each other even if it causes a profit deterioration for both. This is somewhat analogous to classical prisoner's dilemma, attack is the best strategy which cannot earn a best total utility among participated pools. Each pool dispatches own loyal miners as infiltrators to the other pools and they only submit PPoW which does not contribute to a successful mining. A pool employing such infiltrator registers him as a regular miner, so the infiltrator can earn a distributed mining reward. Consequently, the profit of attacking pool become relatively higher than the efforts they made while total utility become lower due to the gap of meaningless work only for PPoWs.

Following the admirable result, various forms of extension have been explored in the literatures taking into account the game theoretic approach. In [26], Courtois et al. analyzed several attacks in which dishonest miners obtain a higher reward than their relative contribution and proposed a new block withholding attack which can maximize the profit of subversive miners. Luu et al. investigated a quantitative analysis of incentive a miner may gain under systematically conducted block withholding attack [27]. They emphasized that the existing pool protocols are susceptible to such attacks by showing the attack is always well-incentivized. Laszka et al. developed a game theoretic model that allows to investigate the long-term viability of attacks against mining pools [28]. They studied a peaceful and one-sided attack equilibria, that is, the conditions under which mining pool has no incentive to launch attack against other pools. Kwon et al. proposed a novel attack namely a fork after withholding (FAW) attack, not just a modified form of block withholding attack but rather a more profitable for attacker in the sense of new Nash equilibrium [29]. Liu et al. applied the evolutionary game theory to analyze the stability for pool selection dynamics by investigating the evolutionarily stable strategy [30]. In [31], Li et al. investigated the robust constrained reachability of networked evolutionary game (NEG) which is effective in dealing with attackers and forbidden profiles. They established a constructive procedure for the robust consensus of NEGs based on algebraic representation. Qin et al. modelled a risk decision problem to study a pool selection problem by adopting the maximum-likelihood criterion under various type of reward mechanisms in one blockchain network [32]. In [33], Wang et al. presented a mining pool selection game modelled by two stages to study a trade-off between the risk of openness of pool and the impact of potential attacks targeting PoW consensus based protocol. Tang et al. proposed a non-cooperative iterated game in terms of zero-determinant (ZD) strategies which can optimize the efficiency of the blockchain network by incentivizing the cooperative miners [34]. They obtained the optimal solution of the maximum system welfare with cooperative miners friendly approach on the quasi-public goods game (PGG).

Most previous works for block withholding attack based on game theory have presented only the result of Nash equilibrium, not the process of pool dynamics. However, to check the feasibility of such theoretic result, the intermediate process is still need to be considered in practice. Therefore, in this paper, we explore the whole mining pool dynamics and build up a practical construction by addressing the detailed process of it. To establish the intermediate process, we mainly investigate the impact of required block size to the revenue with respect to individual miners since it has become an important factor to be considered as the discussion about block size limit controversy became more active such as Bitcoin Cash or SegWit.

Our study not only suggests the detailed manipulation process with proper game theoretic approach, but also arouses a specific attention to the block size limit controversy which is directly related to the practical situation. One of the results supporting the increase in block size concluded that even though there is no block size limit, the unhealthy fee market, i.e., mining larger block size is always beneficial, cannot emerge under the current market economic theories [35]. Each miner has an optimal block size up to their mining power and then mining pool can cover more wider range of block size by controlling revenue trade-off based on mining power, once the block size limit is relaxed. Under such circumstance, the mining pool in our mining game can rig the ESS more easily since the wider the available block size range, the better our manipulation will work. Therefore the results obtained in this work can provide a concrete and practical insight to blockchain standards. The main contributions of this paper are summarized as follows:

- We formalize the mining game based on the PoW consensus to analyze the evolutionary stability. Specifically, in order to apply the block withholding attack, we build a revenue model with the information theory that can reflect the factors which affect our equilibrium including network propagation delay, infiltrating rate, etc.
- To analyze the evolutionary stability, we compute the replicator dynamics of evolutionary game theory. The results give 3 types of stable solution, only one of which will show what we want since the others bring about the vanishing of one pool. Moreover, we give certain conditions for such equilibria.
- Before constructing the intermediate process, we investigate the feasibility of autonomous migration across mining pools according to the previous theoretic results. By adopting the statistics, we approximate the successful mining event into random variable and conclude that the natural migration will rarely occur without an artificial manipulation.
- In order to resolve the previous limitation that individual miners are not expected to move on their own, we construct a manipulation stage in the sense of controlling the revenue model by adjusting the required block size. We allow a better response learning which can migrate a miner with the lowest revenue inductively. We thus conclude our manipulation converges to ESS in finite stages within acceptable block size variations.

The rest of this paper is organized as follows. Section II introduces an overview of common game theoretic concepts. Section III presents the mining game model with concrete problem solving direction step by step. In section IV, we formulate the revenue function of mining pool and solve the evolutionary stability, then establish a better response learning for migrating individual miners inductively. Section V demonstrates numerical results which provide evidences supporting our theoretical discoveries, and finally, we conclude the contents in Section VI.

II. PRELIMINARIES

A. NASH EQUILIBRIA

We can define the mining game as a 3-tuple : $\mathcal{G} = \{\mathcal{N}, S, f\}$, where

- $\mathcal{N}$ is the population of players, $|\mathcal{N}| = n$.
- $S = S_1 \times S_2 \times \cdots \times S_n$ is the set of strategy profiles where S_i is the strategy set for player i.
- f is the strategy-dependent payoff function evaluated at $\mathbf{s} \in S$, i.e., $f(\mathbf{s}) = (f_1(\mathbf{s}), f_2(\mathbf{s}), \cdots, f_n(\mathbf{s}))$, f_i denotes the payoff of player i.

Let s_i be a strategy for player i with $\mathbf{s} = (s_1, \cdots, s_n) \in S$ and let $\mathbf{s}_{-i} := (s_1, \cdots, s_{i-1}, s_{i+1}, \cdots, , s_n)$ be a strategy profile for all players other than player i.

Definition 1 ([36]): A strategy profile $\mathbf{s}^* = \{s_i^*\} \in S$ is a Nash equilibrium (NE) if any unilateral changes of strategy by players lead to undesirably lower utility. That is,

$$\forall i, s_i \in S_i : f_i(s_i^*, \mathbf{s}_{-i}^*) \geq f_i(s_i, \mathbf{s}_{-i}^*). \tag{1}$$

Here,

$$\begin{aligned}(s_i^*, \mathbf{s}_{-i}^*) &= \{s_i^*\} \cup \mathbf{s}_{-i}^* \\ &= \{s_i^*\} \cup (s_1^*, \cdots, s_{i-1}^*, s_{i+1}^*, \cdots, s_n^*) \\ &= (s_1^*, \cdots, s_{i-1}^*, s_i^*, s_{i+1}^*, \cdots, s_n^*) = \mathbf{s}^*\end{aligned} \tag{2}$$

is called a Nash equilibrium and

$$(s_i, \mathbf{s}_{-i}^*) = (s_1^*, \cdots, s_{i-1}^*, s_i, s_{i+1}^*, \cdots, s_n^*) \tag{3}$$

is a dominated strategy of player i with respect to the Nash equilibrium, where the only difference is the strategy of player i. If the inequality (1) holds, player i has no reason to change his strategy and if it holds for every participants in the game, we say a Nash equilibrium is obtained, i.e., no player is willing to change their strategy under any other external factors and can get the optimal utilities.

For $n = 1$, one-player game, it is nothing but an optimization problem, so let us consider the case of $n = 2$. Let a_{ij}, b_{ij} be the payoffs for player 1, 2, respectively, when player 1 uses strategy $i \in S_1$ and player 2 uses strategy $j \in S_2$. Then the payoffs are given by the $n \times m$ matrices as $A = \{a_{ij}\}$, $B = \{b_{ij}\}$ where n, m are the cardinalities of each pure strategies, respectively. When the mixed strategy is allowed, the strategy profile of player 1 can be denoted as $\mathbf{a} = (a_1, \cdots, a_n)^T \in \mathcal{S}_n$, a_i refers to the probability of using strategy $i \in S_1$ and $\mathcal{S}_n$ refers to the unit simplex spanned by the standard unit base. Similarly, if we denote the strategy profile of player 2 as $\mathbf{b} \in \mathcal{S}_m$ with the unit simplex spanned by the standard unit base, the strategy $\mathbf{a} \in \mathcal{S}_n$ is said to be a best reply to $\mathbf{b}$ if

$$\mathbf{c}^T A \mathbf{b} \leq \mathbf{a}^T A \mathbf{b} \tag{4}$$

for all $\mathbf{c} \in \mathcal{S}_n$. In other word, a pair $(\mathbf{a}, \mathbf{b}) \in \mathcal{S}_n \times \mathcal{S}_m$ is a Nash equilibrium if both $\mathbf{a}$ and $\mathbf{b}$ are best replies for each other. One of the most remarkable results of J. F. Nash is that every game with a finite number of players has at least one Nash equilibrium in which each player can use their mixed strategies from the compact, convex, and non-empty set.

B. EVOLUTIONARY DYNAMICS

Nash equilibrium gives a solution of non-cooperative game involving two or more players that no individual can obtain more utility by changing their own strategies. Though it is still a powerful tool to analyze several static games, the limitation was revealed when the game became repetitive and dynamic. That is, in terms of optimization theorem, Nash equilibrium approach only can give local optimal solutions.

For example, the standard prisoner's dilemma shows that both prisoners must defect due to the dominant strategy and the mutual defection is a NE. However, if two players play the game more than once and can remember the opponent's previous action, the iterated prisoner's dilemma became chaotic. If both players know the total number of rounds, the only Nash equilibrium is to always defect. This is very counter-intuitive compared to the standard prisoner's dilemma since both players are aware of the opponent's previous response.

To make them cooperate, the total number of rounds must not be known to them; in this case always defect is still a Nash equilibrium but is no longer a strictly dominant strategy. Tit for tat, responds to cooperate with cooperate and defect with defect, can be an evolutionarily stable status with respect to formal two strategies.

In order to describe the long-term behaviour of the dynamics, we use more fancy tool called a imitation dynamics [37]. There is one simple plausible assumption for game player; to imitate the better. Let x_i be the frequency of type i with n types of strategy. Here, x_i are differentiable functions with respect to time t which represents the growth rate of the population. Let the symmetric payoff matrix A holds all the fitness information for the population with the assumption that the fitness depends linearly upon the population distribution. Then the *replicator equation* yields

$$\dot{x_i} = x_i((A\mathbf{x})_i - \mathbf{x}^T A\mathbf{x}) \tag{5}$$

where $(A\mathbf{x})_i$ is the expected payoff for an individual of type i, and $\mathbf{x}^T A\mathbf{x}$ is the average payoff in the population state $\mathbf{x}$. The replicator equation (5) describes a pool selection process with one rational criteria: more beneficial strategies spread across the whole population, by measuring the surplus of each players. In our model, the replicator equation will be used to estimate the portion of migration among honest miners to reach a stable configuration called a evolutionarily stable strategy (ESS).

The zeros of the equation (5), the rest points of the replicator equation, have interesting properties called as *the folk theorem of evolutionary game theory* [39]:

- if $\mathbf{z}$ is a Nash equilibrium, then it is a rest point
- if $\mathbf{z}$ is a strict Nash equilibrium, then it is asymptotically stable
- if the rest point $\mathbf{z}$ is the limit of an interior orbit, then z is a Nash equilibrium
- if the rest point z is stable, then it is a Nash equilibrium.

An evolutionarily stable strategy, or ESS, is the status that no other minority can invade and confuse the original resident. A strategy used by this invader only leads to the elimination of species unless the size of group is large enough. The replicator equation can be written as

$$\dot{x_i} = x_i[(\mathbf{p}(i) - \mathbf{p}(\mathbf{x}))^T A\mathbf{p}(\mathbf{x})] \tag{6}$$

where $\mathbf{p}(\mathbf{x}) = \sum x_i \mathbf{p}(i)$ is the average strategy within the population, which is an analogue of (5).

Definition 2 ([37]): Let $\mathcal{G} = \{\mathcal{N}, S, f\}$ be a game defined as previous with population state $\mathbf{p}^*$. For some neighborhood $\mathcal{B} \in S$, $\mathbf{p}^*$ is an evolutionarily stable strategy (ESS) if $\forall \mathbf{p} \in \mathcal{B} - \mathbf{p}^*$, the condition $(\mathbf{p} - \mathbf{p}^*)^T A\mathbf{p}^* = 0$ implies

$$(\mathbf{p} - \mathbf{p}^*)^T A\mathbf{p} < 0. \tag{7}$$

Evolutionarily stable strategies were originally motivated from the biological evolution mechanism [37]. With the specific genetic characteristics like heredity or mutation, the behavior of repetitive game players also can be explained by ESS. Based on the imitation protocol, we can predict the population dynamics when a malicious infiltration is in progress. Moreover, we can depict the conditions for stability and pool strategy in terms of the evolutionary game dynamics.

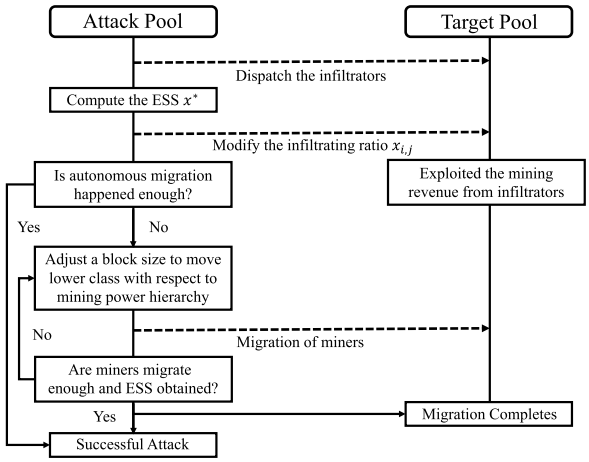

FIGURE 1. Flow chart of evolutionary game model in a blockchain network.

III. SYSTEM MODEL

In this section, we present a mining game model of blockchain network adopting the Nakamoto consensus based on Proof-of-Work (PoW) [1]. According to the result of [25], no-pool-attacks are not Nash equilibria. One tragic equilibrium is composed by malicious infiltrators where attacking other participating pools can earn less than they would have if none had attacked though. This tragedy, namely *the miner's dilemma*, imposes each pool to attack the other unreliable pools. As same as the prisoner's dilemma, even though the superrational strategy in the iterated mining game is to cooperate against a superrational opponent, it is hard to gather whole mining pools into one since the size of major mining pools are too large to unite. We propose such a game model in three steps. The flow chart of our model is described in Fig. 1.

The first step is to formulate the mining game based on the ratio of each pool's loyal miners and infiltrators with the agreement of existence of baleful miners, and to analyze the evolutionarily stable strategy (ESS). One recent research modelled a similar two-stage game whether to open or not the mining pool based on the expected revenue after simultaneous infiltrations [33]. However, frequent opening and closing movement of mining pool may unsettle their own miners in the manner of sustainability. The other research modelled a non-cooperative iterated game with zero-determinant (ZD) strategies, which is also a fancy tool for analyzing the prisoner's dilemma [34]. Even though the ZD strategy is still effective, it is in conflict with our main purpose; we aim to migrate honest miners in a situation where ESS is achieved, but ZD strategy is at most weakly dominant yet be evolutionarily unstable and may be driven to the extinction of one

pool [38], which is the worst situation for our model. Hence, we mainly focus on the flow of mining pool population and the dynamics of ESS with unrelenting block withholding attack.

One important point to consider is how to estimate the infiltrating ratio before computing the ESS. To say the conclusion first, the portion of infiltrators may play a decisive role in the ESS such as the overturn of one dominating mining pool, which detail will be depicted later with numerical analysis on Section V. The case of attacking pool is simple; they themselves can control the portion according to the precomputed ESS up to a reasonable value. However, they cannot estimate the infiltrating portion of targeted opponent pool that either implicitly allowed to attack due to the concealment of malicious attack. Under this lack of information, we assume the opponent side adopts the worst strategy because the increase in infiltrating ratio until just before the collapse of the mining pool results in a positive benefit for the pool. In short, we explore the stability analysis step with fixed infiltrating ratio and give a detailed discussion about change of it later with several numerical results.

The second step is to adjust statistical tools and figure out the characteristic of mining distribution. In general, a block withholding attack is reckoned to be detectable in terms of long-term observation based on the ratio of partial proofs-of-work(PPoWs) and full proofs-of-work(FPoWs). One blind spot is how to measure such insufficient proof-of-work in statistical manner. Blockchain mining is composed by hash functions where the output is expected to behave as independent random variables, which means successful mining events are governed by the laws of statistics. After adapting it to our model, we evaluate the validity for current methodology of tracking malicious infiltrator. For the convenience of computation, we consider two static states of initial phase under innocent and malicious minings.

The last step is to construct the process of migration. If the mining system has several Nash equilibria, there always is a better-response learning that moves the system configuration from any initial equilibrium to a desired equilibrium [40]. Basically miners face a simple problem before mining: where should I mine? The miners are free to choose a mining pool for higher revenue from the coin set, that is, some portion of miners will take a step to improve their own revenue whenever they benefit from changing the pool mined before. Although the infiltrator shares the reward from the attacked pool, it is hard for typical miners to realize that the pool they mined is being attacked in secret. That is, the reality may not follow such theoretic result honestly due to the discrepancy between underlying assumption of fairness of common information and hierarchical structure as an administrator or an individual miner. Our goal is to construct an iterative protocol that moves a game to a desired game theoretical equilibrium with a better response learning by controlling the required block size. The migration process of our model is illustrated in Fig. 2.

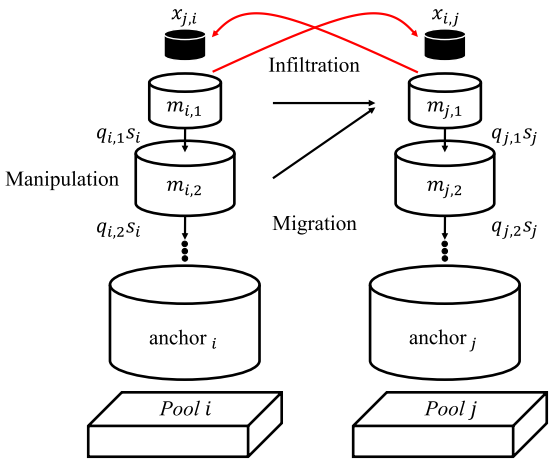

FIGURE 2. Migration process with mining power based hierarchical structure.

IV. MINING GAME ANALYSIS WITH EVOLUTIONARY BLOCK WITHHOLDING ATTACK

In this section, we analyze the evolutionarily stable strategy of mining pool dynamics with an assumption that each pools allow to dispatch own loyal miners as infiltrators adopting a block withholding attack. Moreover, we study a better response learning which migrates the configuration of mining game to the game theoretic equilibrium by enforcing individuals to change their mining pool. The validity for detecting the existence of malicious infiltrator in the view of individual miners may result in a different better response learning, so we estimate a statistical approximation of the mining process before constructing the manipulation step.

A. REVENUE MODEL FORMULATION

Assume that large enough population of N individual mining pools are participated in the blockchain network. As we defined before, consider the mining game $\mathcal{G} = \{\mathcal{N}, S, F\}$ where $\mathcal{N} = \{M_1, M_2, \cdots, M_N\}$ denotes the set of N mining pools with totally $n = |\mathcal{N}| = \sum_{i=1}^{N} |M_i|$ individual miners, $S = S_1 \times S_2 \times S_n$ denotes the set of strategy profiles, and $f = (f_1, f_2, \cdots, f_n)$ denotes the payoff of miners depends on the strategy profile $\sigma \in S$. In our model, the strategy profile σ is consistent as every mining pools choose to attack other pools. In fact, this choice is somewhat natural for large pools since it became harder to counteract against malicious infiltrators as the pool size become larger, moreover that is the static Nash equilibrium for PoW consensus [25]. Let h_i be the required individual hash rate for joining pool i and x_i be the miners' population fraction in pool i, i.e., $\sum_{i\in\mathcal{N}} x_i = 1$ with $\forall i, x_i \geq 0$. According to the Nakamoto consensus, the chance of mining a new block is proportional to individual hash rate for solving PoW problem [41]. Without attacks, the probability of successful one round mining for pool i is then

$$\Pr_i^{\text{without}}(\mathbf{x}, \mathbf{h}) = \frac{h_i x_i}{\sum_{j=1}^{N} h_j x_j}, \tag{8}$$

where $\mathbf{x} = \{x_1, \cdots, x_N\}$ and $\mathbf{h} = \{h_1, \cdots, h_N\}$ are the configurations of population fraction and required hash rates in whole network, respectively.

Now let $x_{i,j}$ be the population fraction of infiltrators from pool i to pool j. These infiltrators cannot positively contribute the successful mining rate while they get some reward from the target pool, since they just waste the mining power trying to find only PPoWs which are useless in comparison with FPoW. In other word, for the pool i, $\sum_{k\neq i} x_{i,k}$ is nothing but the loss portion of work in the view of total network. Then, by adapting it to (8), the malicious attack changes the success probability as

$$\Pr_i^{\text{with}}(\mathbf{x}, \mathbf{h}, \mathbf{h}^-) = \frac{h_i(x_i - \sum_{k\neq i} x_{i,k})}{\sum_{j=1}^{N} h_j(x_j - \sum_{k\neq j} x_{j,k})}. \tag{9}$$

where $\mathbf{h}^- = \{x_{i,j}\}_{i\neq j\in\mathcal{N}}$ is the configuration of population fraction of infiltrators. One observation that the attacked pool has higher success probability than attacking pool provides a rational reason how the reward from infiltration covers the loss of mining power.

During the mining phase, pool i must broadcast the solution to its neighborhoods after solving a crypto puzzle for disseminating their mined block to the entire blockchain network. Since the mining events can be seen as a random event in the sense of hash function, sometimes the situation called *a fork* that several mining pools discover a new block simultaneously can occur. Unfortunately, the only block propagated their solution to the most of network for the first time will be confirmed as the new head block even though the others also reach a consensus. To deal with such unfavorable accidents, we consider a propagation probability as an important factor and follow the process of [34]. A few empirical studies support that the transmission delay and the transaction verification time between each nodes mainly determine the block propagation time [41], [42]. Shannon-Hartley theorem states the theoretical upper bound on the information rate of data that can be transmitted at any arbitrarily low error rate, and by virtue of the power series a lower bound of channel's carrying capacity c can be approximated as

$$\Delta\tau_d(s) = \tau_d(s) - \tau_d(0) \approx \frac{s/\gamma}{c} \tag{10}$$

where τ_d is the block transmission delay, s is the block size, and γ is the network-related parameter named coding gain [41]. The block verification time is nothing but a linear function of block size since verifying a block requires almost same time regardless of hash string, i.e., $\tau_v(s) = bs$ where b is the average verification speed. Consequently, we get a propagation delay as

$$\tau(s) = \Delta\tau_d(s) + \tau_v(s) = \frac{s/\gamma}{c} + bs. \tag{11}$$

The proof-of-work propagation can be seen as a Poisson process [43], therefore the time difference governed by an exponential distribution. After combining (10) and (11) with the approximation of Andresen [44], the orphaning probability, or the incidence of discarding, can be written as

$$\Pr^{\text{orphan}} = 1 - e^{-\tau(s)/T} = 1 - e^{-(\frac{s/\gamma}{c} + bs)/T}, \tag{12}$$

where T is an average mining time such as 600s in Bitcoin as widely known [1].

Finally, a total revenue in one round contains not only the fixed reward of currently mined block and the extra transaction fee, but the shared rewards of previous rounds from the other pools gathered by own infiltrators. One caution is that the expedition reward cannot be distributed immediately. If not, honest miners may doubt their unsubstantiated reward sharing while the pool they worked didn't mined successfully yet. Thanks to the result in [25], the pool revenue with consecutive infiltration reward converges, that is we may consider a revenue in one round already includes such external rewards. Moreover, the transaction fee is a linear function of each required block size s_i, so the total revenue in one round can be written as $R_0 + rs_i$ where R_0 is the fixed mining reward and r is the transaction fee per unit block size. For the convenience of computation, we assume that the effect of transaction fee is consistent with fixed s_i and just denote the whole revenue as R. The pool can earn a mining reward when they 1) successfully find a block and 2) propagate it to whole network, i.e., mined block orphaning does not happened. Expectation of revenue is the product of total revenue, success probability for both mining and propagation with subtraction on the sunk cost, therefore by joining (9) and (12) together, our mining revenue for pool i under configurations of population fraction $\mathbf{x}$, required hash rates $\mathbf{h}$, and population fraction of infiltrators $\mathbf{h}^-$ can be formulated as

$$\begin{aligned} E_i(\mathbf{x}, \mathbf{h}, \mathbf{h}^-) &= R \cdot \Pr_{\text{success}} \cdot (1 - \Pr^{\text{orphan}}) - ph_i \\ &= R \cdot \Pr_i^{\text{with}}(\mathbf{x}, \mathbf{h}, \mathbf{h}^-) e^{-\tau(s)/T} - ph_i \end{aligned} \tag{13}$$

where ph_i refers to an electricity charge of mining machine querying hash strings with unit price p as a sunk cost.

TABLE 1. Major parameters.

Symbol	Definition
x_i	Population fraction of pool i
$x_{i,j}$	Infiltrating rate from pool i to j
h_i	Hash rate of pool i
τ	Propagation delay
s_i	Block size of pool i
T	Average mining time
R	Mining reward
r	Transaction fee per unit block size
p	Unit electricity charge per hash rate
q	Ratio of changed block size
N_i	Population size of pool i

B. EVOLUTIONARILY STABILITY ANALYSIS

From this subsection, we study a special competitive blockchain network with two mining pools $\mathcal{N} = \{P_1, P_2\}$. Since individual miners want to maximize their net profit

and are willing to transfer their mining pool depends on the revenue, it is natural to solve an ordinary differential equation with respect to the population. Let $(x_1, x_2) = (x, 1-x)$ be the population fractions of pool 1, 2 with positive x and denote y_i the expected revenue of pool i. In this case, the replicator equation (5) became fairly simple as

$$\begin{aligned} \dot{x_1} &= x_1((A\mathbf{x})_1 - \mathbf{x}^T A\mathbf{x}) \\ &= x_1(y_1 - \bar{y}) = x_1(1-x_1)(y_1 - y_2). \end{aligned} \tag{14}$$

Also, our revenue model (13) became

$$\begin{cases} y_1 = \dfrac{h_1(x_1 - x_{1,2})}{h_1(x_1 - x_{1,2}) + h_2(x_2 - x_{2,1})} \cdot Re^{-\tau(s)/T} \\ [4pt] \qquad\qquad - ph_1(x_1 - x_{1,2}), \\ y_2 = \dfrac{h_2(x_2 - x_{2,1})}{h_1(x_1 - x_{1,2}) + h_2(x_2 - x_{2,1})} \cdot Re^{-\tau(s)/T} \\ [4pt] \qquad\qquad - ph_2(x_2 - x_{2,1}). \end{cases} \tag{15}$$

For convenience, if we define as

$$c_1(x_1, x_2) = h_1(x_1 - x_{1,2}) + h_2(x_2 - x_{2,1}), \tag{16}$$

$$c_2(x_1, x_2) = h_1(x_1 - x_{1,2}) - h_2(x_2 - x_{2,1}), \tag{17}$$

we can state Theorem 1 as follows.

Theorem 1: Consider the game $\mathcal{G} = \{\mathcal{N}, S, f\}$ with two mining pools modeled by the payoff function (15), where both pools intend to infiltrate their own miners into each other for the relatively high utility based on the *miner's dilemma*.

1) The boundary states $(x_1, x_2) = (1, 0)$ or $(0, 1)$ are ESSs if the conditions

$$h_1(1 - x_{1,2}) - h_2 x_{2,1} < \frac{R}{p} e^{-\tau(s)/T}, \tag{18}$$

$$h_2(1 - x_{2,1}) - h_1 x_{1,2} < \frac{R}{p} e^{-\tau(s)/T} \tag{19}$$

hold, respectively.

2) Without loss of generality, suppose pool 1 requires more hash rate than pool 2, i.e., $h_1 > h_2$. The non-trivial rest point of replicator equation (14) is given by $(x_1, x_2) = (x^\star, 1 - x^\star)$ where

$$x^\star = \frac{1}{h_1 - h_2}(h_1 x_{1,2} - h_2(1 - x_{2,1}) + \frac{R}{p} e^{-\tau(s)/T}), \tag{20}$$

and it is an ESS if the both conditions

$$1 - \frac{2h_2}{c_1}(x_2 - x_{2,1}) > 0, \tag{21}$$

$$1 - \frac{4h_1 h_2}{c_1^2}(x_1 - x_{1,2})(x_2 - x_{2,1}) < 0 \tag{22}$$

hold. Moreover, $x^\star$ is the unique globally stable point and it is the only Nash equilibrium in game $\mathcal{G}$.

Proof: By the definition 2 and the folk theorem of evolutionary game theory in section II, it is enough to find the asymptotically stable state of the replicator equation (14). At the rest point $\mathbf{x}$ in the (14), $(A\mathbf{x})_1 - \mathbf{x}^T A\mathbf{x}$ refers to eigenvalues for the Jacobian whose stability can be evaluated depending on its corresponding eigenvector. That is, a rest point $\mathbf{x}$ is an ESS if all its eigenvalues have negative real parts, or equivalently, the Jacobian matrix is negative definite. Rewrite our target ODE:

$$\begin{aligned} f(x_1, x_2) &= x_1(1 - x_1)(y_1 - y_2) \\ &= x_1(1 - x_1)\left\{\frac{c_2}{c_1} Re^{-\tau(s)/T} - pc_2\right\}. \end{aligned} \tag{23}$$

The entries of Jacobian can be derived by some tedious calculations:

$$\begin{cases} \dfrac{\partial f_1}{\partial x_1} = \left\{(1-2x_1)\dfrac{c_2}{c_1} + x_1(1-x_1)\dfrac{2h_1h_2(x_2 - x_{2,1})}{c_1^2}\right\} Re^{-\dfrac{\tau(s)}{T}} \\ \qquad -p\{(1-2x_1)c_2 + x_1(1-x_1)h_1\}, \\ \dfrac{\partial f_1}{\partial x_2} = x_1\left\{\dfrac{c_1c_2 - 2x_2h_1h_2(x_1 - x_{1,2})}{c_1^2} Re^{-\dfrac{\tau(s)}{T}} \right. \\ \qquad \left. -p(c_2 - x_2h_2)\right\}, \\ \dfrac{\partial f_2}{\partial x_1} = -x_2\{\dfrac{c_1c_2 + 2x_1h_1h_2(x_2 - x_{2,1})}{c_1^2} Re^{-\dfrac{\tau(s)}{T}} \\ \qquad -p(c_2 - x_1h_1)\}, \\ \dfrac{\partial f_2}{\partial x_2} = \left\{(2x_2-1)\dfrac{c_2}{c_1} + x_2(1-x_2)\dfrac{2h_1h_2(x_1 - x_{1,2})}{c_1^2}\right\} Re^{-\dfrac{\tau(s)}{T}} \\ \qquad +p\{(1-2x_2)c_2 - x_2(1-x_2)h_2\}. \end{cases} \tag{24}$$

On the boundary rest point $(1, 0)$, the corresponding Jacobian matrix looks more clear,

$$J|_{(1,0)} = \begin{bmatrix} -\dfrac{c_2}{c_1} Re^{-\tau(s)/T} + pc_2 & \dfrac{c_2}{c_1} Re^{-\tau(s)/T} - pc_2 \\ 0 & -\dfrac{c_2}{c_1} Re^{-\tau(s)/T} + pc_2 \end{bmatrix} \tag{25}$$

which is an upper triangular form. It is easy to see that the corresponding eigenvalues are diagonal entries, that is, repeated $-\frac{c_2}{c_1} Re^{-\tau(s)/T} + pc_2$. To guarantee the negative definiteness of Jacobian (25), we get (18) by simply substituting $\mathbf{x} = (1, 0)$. In a similar manner, we can get (19) for the case of $\mathbf{x} = (0, 1)$. Hence, the proof of first part is done.

On the other hand, the nontrivial rest point of (23) can be obtained from $\frac{c_2}{c_1} Re^{-\tau(s)/T} - pc_2 = 0$, which coincides to the

solution (20). Again by some tedious calculations,

$$\begin{cases} J_{11} = (1-2x_1)pc_2 + x_1(1-x_1)\cdot 2h_1h_2(x_2-x_{2,1})\dfrac{p}{c_1} \\ \quad -p\{(1-2x_1)c_2 + x_1(1-x_1)h_1)\} \\ \quad = px_1(1-x_1)h_1\left\{\dfrac{2h_2}{c_1}(x_2-x_{2,1})-1\right\}, \\ J_{12} = x_1\left\{pc_2 - \dfrac{2h_1h_2x_2(x_1-x_{1,2})}{c_1c_2}pc_2 - pc_2 + px_2h_2\right\} \\ \quad = px_1x_2h_2\left\{1-\dfrac{2h_1}{c_1}(x_1-x_{1,2})\right\}, \\ J_{21} = x_2\left\{pc_2 + \dfrac{2h_1h_2x_1(x_2-x_{2,1})}{c_1c_2}pc_2 - pc_2 + px_1h_1\right\} \\ \quad = px_1x_2h_1\left\{1+\dfrac{2h_2}{c_1}(x_2-x_{2,1})\right\}, \\ J_{22} = -(1-2x_2)pc_2 - x_2(1-x_2)\cdot 2h_1h_2(x_1-x_{1,2})\dfrac{p}{c_1} \\ \quad +p\{(1-2x_2)c_2 - x_2(1-x_2)h_2\} \\ \quad = -px_2(1-x_2)h_2\left\{\dfrac{2h_1}{c_1}(x_1-x_{1,2})+1\right\}, \end{cases}$$

where $J|_{(x^\star,1-x^\star)} = \begin{bmatrix} J_{11} & J_{12} \\ J_{21} & J_{22} \end{bmatrix}$ is the corresponding Jacobian matrix. Moreover,

$$\begin{aligned} \det(J) &= J_{11}J_{22} - J_{12}J_{21} \\ &= 2x_1^2x_2^2p^2h_1h_2\left\{\frac{4h_1h_2}{c_1^2}(x_1-x_{1,2})(x_2-x_{2,1})-1\right\} \end{aligned} \tag{26}$$

gives a required condition for ESS. To be an asymptotically stable rest point, negative definiteness forces $J_{11} < 0$ and $\det(J) > 0$, which are exactly (21) and (22).

The remaining part is to show a global stability. Note that our revenue model (23) has 1 discontinuity and 2 tangent points, indeed our ODE is a typical Lyapunov function. Thus, our ESS is an asymptotically stable and an interior ESS $(x^\star, 1-x^\star)$ is globally stable [45]. One can easily check that the discontinuity $c_1 = 0$ is not in [0, 1] by (21) as

$$c_1 > 2h_2(x_2 - x_{2,1}) > 0 \tag{27}$$

since $0 < x_{2,1} < x_2$ by the definition of $x_{2,1}$.

□

Remark 1: The replicator dynamics of $N = 2$ case admits only three outcomes; no interior point, stable interior point, and unstable interior point. If the interior point exists and is globally stable, it is the only Nash equilibrium whose corresponding strategy is called a *stable coexistence*.

The boundary states $(x_1, x_2) = (1, 0)$ or $(0, 1)$ are not the desirable results to mining pool even though they are ESSs. For instance, $(x_1, x_2) = (1, 0)$ indicates the collapse of pool 2, consequently the infiltrators of pool 1 loses a host for exploiting mining revenue and they should go back to pool 1. Hence, the utilities of both mining pool and infiltrator decrease; mining pool cannot earn the extra revenue with no-full-exertion by dispatching own miner, and the infiltrators have to put their whole mining power honestly to get the reward from originally affiliated mining pool.

One situation that the mining pool may worry about is an unexpected deviation of infiltrator who was prescribed to follow the evolutionarily stable strategy. As we discussed above, the infiltrators have no reason to adopt the defiant behavior unless they are not rational players of mining game. If they are real antagonists and act a hostile behavior with some reason, the mining pool must respond immediately before facing a difficult situation. The first case is the infiltrator underestimating himself to deceive the original pool, i.e., $x_{1,2}$ became smaller than required. This case is partially related to the main result of FAW attack [29]; it does not harm the ESS critically but the attacking pool may get lower extra revenue from the target pool. Unfortunately, as block withholding attack does, there is no concrete and effective solution yet to our best knowledge. The second case is performing more than prescribed mining power to the target pool, i.e., $x_{1,2}$ became larger than required. Then the ESS falls into the conditions either (18) or (19), which results very dangerous situation of vanishing of pool 2. Unlike the first case, the second case can identify the indication by steady checking of target pool's population. Therefore the proper remedies should be taken such as reducing the portion of infiltrators with tracking such antagonists down. The detailed discussion of latter case will be handled at section V with numerical figures.

C. STATISTICAL DISTINGUISHABILITY

The argument studied at the previous subsection only works when the game is fair, that is, every game player must know whole information and strategic background of pools. One mismatch of our intended infiltration game with block withholding attack is, honest miner needs to be moved depends on the result of replicator dynamics while the fundamental reason of migration is still concealed. From the point of view of mining pools, publicly known infiltrators may harm their own loyal miners so it is hardly possible to admit the existence of malicious action. In this subsection, we study whether honest miners may obey the theoretical ESS in the lack of information or not.

In the case of miners, the main motivation of migration comes from the revenue. This revenue is directly related to the successful mining rate of crypto puzzle and since PoW consensus requires to solve a hash problem on the certain condition, each mining trials act like random variables.

Lemma 1: Let $\{X_{j,i}\}_{i\in\mathbb{N}}$ be a sequence of independent and identically distributed random variables which refers the mining event of ith miner in pool j, that is, $X_{j,i} = 1$ if a miner i finds the hash solution. Then the successful mining rate of pool j can be approximated by normal distribution whose the mean is approximately equal to its variance.

Proof: First of all, we assume that the influence of temporary change of mining pool population is minor. Also note that the consecutive mining events are independent due to the characteristic of hash function.

As we saw at (8), the expected mining rate K_i of pool i is proportional to h_ix_i. If a winning block computes a hash with exactly k zeros, we may say that the total trial is

$m = K_i \cdot 2^k$ by brute force and the randomness of hash function forces the expectation as $\mu = 2^{-k}$. Let X_j denotes the mining probability of miner j and P_l denotes the probability mass function, then

$$\begin{aligned} Var(X_j) &= \sum_{l=1}^{m} P_l(x_l - \mu)^2 \\ &= \mu(1-\mu)^2 + (1-\mu)(0-\mu)^2 \\ &= \mu(1-\mu). \end{aligned} \tag{28}$$

Indeed, $X_1 + \cdots + X_m$ is also a normal distribution with $N(m\mu, m\mu(1-\mu))$. □

Remark 2: The result of Lemma 1 agrees to the previous discussion of (12), that is, the mining event can be approximated by Poisson process. It is well-known that the binomial distribution converges toward the Poisson distribution.

Theorem 2: Suppose the expected number of mined block is a linear function of hash rate. In the game $\mathcal{G} = \{\mathcal{N}, S, f\}$ with two mining pools, the successful mining rates 1) with infiltrator and 2) without infiltrator are statistically close in a short term, i.e., individual miners cannot recognize the existence of external attack.

Proof: We focus on the honest miner of pool 1 without loss of generality. By the Lemma 1, each step of mining game can be approximated by normal distribution. Let $\mathcal{D} = N(\mu, \sigma^2)$ and $\mathcal{D}_0 = N(\mu_0, \sigma_0^2)$ be such distributions of with and without infiltrator, respectively. Since the expected mining rate is proportional to $h_i x_i$ and $\mu_0 \approx \sigma_0^2$ holds, we may say

$$\mathcal{D}_0 = N\big(d_1 h_1(x_1 - x_{1,2}), d_2\sqrt{h_1(x_1 - x_{1,2})}\big) \tag{29}$$

for some constants $d_1, d_2 > 0$. For pool 1, the infiltrator from pool 2 believed to work honestly brings a positive benefit and

$$\mu = d_1(h_1(x_1 - x_{1,2}) + h_2 x_{2,1}), \tag{30}$$
$$\sigma = d_2\sqrt{h_1(x_1 - x_{1,2}) + h_2 x_{2,1}} \tag{31}$$

are two parameters of $\mathcal{D}$.

To measure the amount of overlap between two statistical samples, we calculate the statistical distance. For multivariate normal distributions $\mathcal{D}_i = N(\mu_i, \Sigma_i)$, the Bhattacharyya distance is defined as

$$D_B = \frac{1}{8}(\mu_1 - \mu_2)^T \Sigma^{-1}(\mu_1 - \mu_2) + \frac{1}{2}\ln\Big(\frac{\det \Sigma}{\sqrt{\det \Sigma_1 \det \Sigma_2}}\Big), \tag{32}$$

where $\Sigma = (\Sigma_1 + \Sigma_2)/2$. In our case of $|\mathcal{N}| = 2$, the distance is

$$D_B = \frac{1}{4}\Big(\frac{(\mu - \mu_0)^2}{\sigma^2 + \sigma_0^2}\Big) + \frac{1}{4}\ln\Big\{\frac{1}{4}\Big(\frac{\sigma_0^2}{\sigma^2} + \frac{\sigma^2}{\sigma_0^2} + 2\Big)\Big\}. \tag{33}$$

We claim that D_B is a negligible function. The first term is

$$\frac{1}{4} \cdot \frac{d_1 h_2^2 x_{2,1}^2}{2h_1(x_1 - x_{1,2}) + h_2 x_{2,1}} = \frac{1}{\text{poly}(x_1)},$$

and in the second term,

$$\frac{\sigma_0^2}{\sigma^2} = 1 + \frac{-h_2 x_{2,1}}{h_1(x_1 - x_{1,2}) + h_2 x_{2,1}},$$
$$\frac{\sigma^2}{\sigma_0^2} = 1 + \frac{h_2 x_{2,1}}{h_1(x_1 - x_{1,2})}$$

infer the logarithm converges to 0 since

$$\lim_{x_1 \to \infty} \frac{1}{h_1(x_1 - x_{1,2})} - \frac{1}{h_1(x_1 - x_{1,2}) + h_2 x_{2,1}} = 0.$$

Therefore, $\mathcal{D}$ and $\mathcal{D}_0$ are statistically close. □

Remark 3: In a long term, the infiltrating rate $x_{1,2}$ and $x_{2,1}$ are no more constants. As the result of Theorem 1, the solution of replicator equation (20) implies that x^* is a linear function of $x_{1,2}$ and $x_{2,1}$. Furthermore, $D_B = \text{poly}(x_1)$ results a meaningful difference between initial state and ESS state of game $\mathcal{G}$.

D. MOVING BETWEEN EQUILIBRIA

Theorem 2 refers that unless the portion of infiltrator is large enough, it is hard to expect the individual miners to migrate mining pool on their own. Furthermore, increasing the number of infiltrators up to notable portion at once is even risky since it may harm the loyalty of honest miners. In this subsection, we suggest a somewhat gentle reward model which avoids both of the mentioned problems.

The main idea of our artificial manipulation is based on a *better response learning*. For the configuration $\mathbf{s} \in S$ with payoff function f, a move from $\mathbf{s} = (s_i, \mathbf{s}_{-i})$ to $\mathbf{s}^* = (s_i^*, \mathbf{s}_{-i})$ is a better response step for miner i if $f(\mathbf{s}) < f(\mathbf{s}^*)$, and a better response learning is a sequence of configurations in better response step. Our main claim is the revenue per unit (RPU) with respect to hash rate is an ordinal potential for a game $\mathcal{G}$, and it has a better response learning further. After constructing a better response step, we conclude that our reward model converges to the required ESS state.

Note that $h_i x_i$, the mining power of pool i, is an average value. Definitely major mining group of one pool has overwhelming computing power than individual miners, and our proposal is to move such 'minor' while 'major' is still mining in original pool by changing reward. Consider the ordered set $\langle P_1, \prec \rangle$ where $\prec$ is a partial order with respect to mining power. For the convenience, we divide P_1 into two groups as the *mover* of size N_m and the *anchor* of size N_a with $N_1 = N_m + N_a$. It is natural to assume $N_m < N_a$, and suppose the average mining power of anchor is k times better than the mover's.

The easiest way to control the revenue is changing the block size s_i. Even though we assumed every circumstances are equally regulated except the required hash rate for calculating the ESS configuration, the mining game $\mathcal{G}$ performs billions of operations per hour and pool population fluctuates frequently. Thus, an exact equality on parameter setting is undesirable, i.e., $\mathcal{G}$ is a generic game and the expected reward differs. As we discussed at the model formulation step, we set

the total reward as $R_0 + rs_i$ where R_0 is the fixed mining reward and r is the transaction fee per unit block size. Then the initial RPU of mover can be written as

$$RPU_{m,s_1} = \frac{1}{N_1 c_1}(R_0 + rs_1)e^{-\tau(s_1)/T} - p. \tag{34}$$

If the pool 1 changes the size of mining block with rate q, we get

$$RPU_{m,qs_1} = \frac{1}{N_1 c_1}(R_0 + rqs_1)e^{-\tau(qs_1)/T} - p. \tag{35}$$

As the function of s_i, the unique global maximum of RPU is

$$\frac{\partial}{\partial s}RPU_{m,s} = 0 \Leftrightarrow s^* = \frac{T}{\tau} - \frac{R_0}{r} \tag{36}$$

For $s_1 > s^*$, $RPU_{m,s_1} > RPU_{m,qs_1}$ if $q \geq 1$ and this is intuitively reasonable because increasing the block size also increases the burden for miners. If the mover migrates to pool 2, the new RPU is

$$RPU'_{m,s_2} = \frac{1}{(N_2 + N_m)c_1} \cdot \frac{h_1}{h_2}(R_0 + rs_2)e^{-\tau(s_2)/T} - p. \tag{37}$$

We may assume the initial state was stable with respect to mover, that is (34) and (37) are in balance. Then we get $RPU'_{m,s_2} > RPU_{m,qs_1}$ and the mover has an advantage to migrate if the pool 1 requires larger block size. Denote $\Delta_{\chi,t} = RPU_{\chi,ts_1} - RPU'_{\chi,s_2}$ with $\chi \in \{a, m\}$, then $\Delta_{m,1} = 0$ and $\Delta_{m,q} < 0$.

On the other hand, in a similar manner,

$$RPU_{a,s_1} = k \cdot RPU_{m,s_1},\ RPU_{a,qs_1} = k \cdot RPU_{m,qs_1}, \tag{38}$$

$$RPU'_{a,s_2} = \frac{k}{(N_2 + N_a)c_1} \cdot \frac{h_1}{h_2}(R_0 + rs_2)e^{-\tau(s_2)/T} - pk. \tag{39}$$

First, the anchor is also in a stable configuration:

$$\begin{aligned}\Delta_{a,1} &= k(RPU_{m,s_1} - \frac{N_2 + N_m}{N_2 + N_a}RPU'_{m,s_2}) \\ &> k \cdot \Delta_{m,1} = 0\end{aligned} \tag{40}$$

implies the anchor gets more revenue for mining at pool 1. Now we claim that the anchor need not to have an advantage of migrating:

$$\Delta_{a,q} = k(RPU_{a,qs_1} - \frac{N_2 + N_m}{N_2 + N_a}RPU'_{a,s_2}) \tag{41}$$

is still non-negative while $\Delta_{m,q} < 0$ under certain circumstance.

Theorem 3: There is a better response learning on $\mathcal{G}$, i.e., $RPU_{\chi,s}$ is an ordinal potential and can make the mover to migrate while the anchor stays by adjusting total revenue.

Proof: By the above arguments, it is enough to show $\exists q^* > 1$ such that $\Delta_{a,q^*} \geq 0$. Let

$$g(s) = \frac{N_2 + N_m}{N_2 + N_a}(R_0 + rs)e^{-\tau(s)/T}, \tag{42}$$

then

$$\Delta_{a,q} \geq 0 \Leftrightarrow (R_0 + rqs_1)e^{-\tau(qs_1)/T} \geq g(s_1). \tag{43}$$

To solve the equality, we use the Lambert W function which is an inverse of $f(z) = ze^z$:

$$q^* = -\frac{T}{\tau s_1}W\big(-\frac{\tau}{rT}g(s_1)e^{-\frac{\tau R_0}{rT}}\big) - \frac{R_0}{rs_1}. \tag{44}$$

By the characteristic of Lambert W function, we may say that $W(ze^z) \leq -1$ with corresponding $-1/e \leq ze^z < 0$, which guarantees the injectivity. Consequently, the W function part is

$$\begin{aligned}&W\big(-\frac{\tau}{rT} \cdot \frac{N_2 + N_m}{N_2 + N_a}(R_0 + rs_1)e^{-\frac{\tau}{rT}(R_0 + rs_1)}\big) \\ &< W\big(-\frac{\tau}{rT}(R_0 + rs_1)e^{-\frac{\tau}{rT}(R_0 + rs_1)}\big) \\ &= -\frac{\tau}{rT}(R_0 + rs_1)\end{aligned} \tag{45}$$

by the assumption $N_m < N_a$ and W is a monotone decreasing function on $z \leq -1$. Hence,

$$q^* > -\frac{T}{\tau s_1} \cdot (-\frac{\tau}{rT}(R_0 + rs_1)) - \frac{R_0}{rs_1} = 1 \tag{46}$$

and we can find such q^* satisfies $q^* > 1$. Therefore, we get $\Delta_{a,q^*} \geq 0$ and this completes the argument by increasing the required block size of pool 1 as $q^* s_1$. □

Remark 4: The condition $W(ze^z) \leq -1$ sometimes is denoted as W_{-1} alternatively. In particular, the equality case $W_{-1} = -1$ on (44) satisfies

$$q^* = \frac{T}{\tau s_1} - \frac{R_0}{rs_1} = \frac{s^*}{s_1} < 1, \tag{47}$$

which converts RPU_{m,s_1} to RPU_{m,s^*}. Since s^* is an optimal block size for global maximum with respect to the mover by (36), this action only binds them more tightly in pool 1.

Now, we inductively applying Theorem 3. In the set of anchor, there is still a relative power order. If we define a set $\{RPU_{m_j,s} | m_j \in P_1, j \in \mathbb{N}\}$ ordered lexicographically from smallest to largest RPU, we can find a maximal index j_0 such that $\sum_{j=1}^{j_0} |m_j| \leq (1 - x^*)|P_1|$ where x^* is an evolutionarily stable portion of total anchors of pool 1, which can be derived from Theorem 1. Since P_1 is a finite set, our inductive step completes in a finite number of iteration j_0 and the remaining population $x^*|P_1|$ converges to ESS.

Remark 5: A concrete estimation of q^* is independent to the infiltrating rate. $x_{i,j}$ only determines the equilibrium state $(x^*, 1 - x^*)$ of populations.

Corollary 1: Revenue manipulation scheme with better response learning in Theorem 3 converges to a required ESS configuration in finite steps. That is, the mining pool can rig the system from initial to a desired ESS state by controlling block size s_i.

V. NUMERICAL ANALYSIS

In this section, we analyze the mining game $\mathcal{G}$ by presenting numerical simulations. In order to verify our mathematical discussion, we investigate our model step by step. Consider a blockchain network with $N = 2$ under generic game assumption, that is, no two pools provide exactly same revenue.

Algorithm 1 Inductive Manipulation Toward an ESS

Require: $R_{\prec} = \{RPU_{m_j,s} | m_j \in P_1, j \in \mathbb{N}\}$

1: $j \leftarrow 1$
2: compute the number of expected iterations j_0
3: **repeat**
4: find a minimal q such that $RPU_{m_j,qs_1} < RPU'_{m_j,s_2}$ and $RPU_{c_{j+1},qs_1} \geq RPU'_{c_{j+1},s_2}$
5: set the required block size s_1 to qs_1
6: allow better response learning and make only lower class m_j migrates while higher class m_{j+1} stays
7: **until** $j = j_0$

TABLE 2. Constants used in stability analysis.

Parameter	Value
Total population	$n = 1000$
Unit electricity charge per hash rate	$p = 0.1$
Required block size	$s = 10$
Average mining time	$T = 600$
Propagation delay	$\tau = 20$

First of all, we demonstrate the evolutionary dynamics of our revenue model $E_i(\mathbf{x}, \mathbf{h}, \mathbf{h}^-)$ in (13). As we discussed at Remark 1, there are totally 3 types of solutions in replicator equation with two pools. The ESS condition x^* is determined by several parameters, but R, p, s, T, τ acts as one constant so we fix $p = 0.1, s = 10, T = 600, \tau = 20$ and control R only for convenience.

Fig. 3 shows the *dominating* strategy of pool 1 under initial state $(x_1, x_2) = (0.7, 0.3)$, $(x_{1,2}, x_{2,1}) = (0.05, 0.03)$, $(h_1, h_2) = (2, 1)$ and $R = 6$. The inequality (18) holds and results a whole vanishing of relatively weak pool 2. On the other hand, Fig. 4 shows the *stable coexistence* strategy of pool 1 and pool 2, that is, populations of both pool converge to some interior point $(x^*, 1 - x^*)$ which is approximately $(0.357, 0.643)$ in our parameter setting. The only changed parameter is smaller mining reward $R = 2$. We can check the same aspect when the mining reward is fixed as $R = 6$ but the required hash rates increased to $(h_1, h_2) = (4, 2)$. This provides a strong evidence that the ratio of mining reward to mining power acts as an important factor of evolutionary stability. Notice that the mining power also involves the infiltrating rate $x_{i,j}$ as of forms $h_i(1 - x_{i,j})$ or $x_i - x_{i,j}$, and we will discuss it more precisely soon. In practice, dominating strategy is undesirable and rarely happens; the only possibility is due to its relatively low competitiveness, and such pools fell behind by natural selection at a very early stage. Then our main interest is on a stable coexistence strategy, that is, how to artificially relocate miners and lead to interior ESS by assigning infiltrators.

Fig. 5 illustrates the variation of population ratio dynamics on dominating strategy for pool 1. Unless the initial population is 0, our revenue model is guaranteed to converge to some ESS as in the first three cases $x_1 = 0.8, 0.5$, and 0.3. As we mentioned at the previous analysis, the ratio of mining reward to mining power mainly determines the

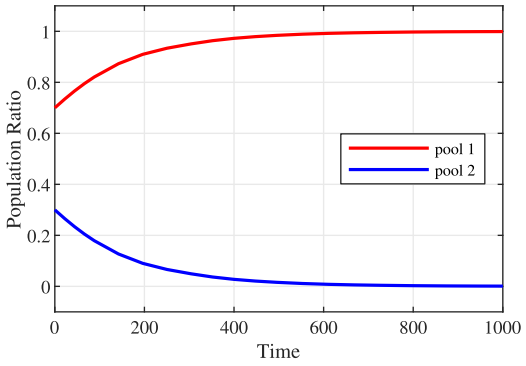

FIGURE 3. Stable with no interior equilibrium for $(x_1, x_2) = (0.7, 0.3)$ and $x^* = 1$, pool 1 ***dominates*** pool 2.

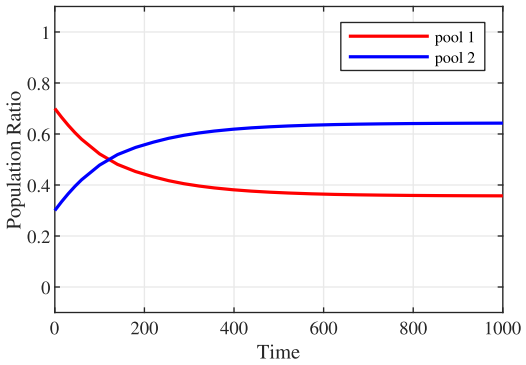

FIGURE 4. Globally stable interior equilibrium for $(x_1, x_2) = (0.7, 0.3)$ and $0 < x^* < 1$, ***stable coexistence***.

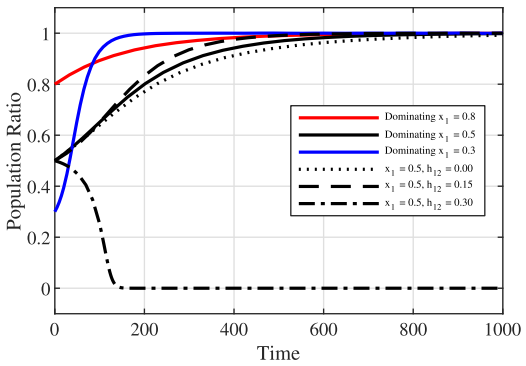

FIGURE 5. Convergence of ***dominating*** strategies with respect to x_1.

end state of ESS. When $x_1 = 0.3$, which is relatively poor than $x_2 = 0.7$, it is easy to converge to the lower end as long as pool 1 does not take strong actions. One solution is to make the mining power competitive by increasing h_1, and we get such population dynamic by taking $R = 15$ and $h_1 = 4$ while $h_2 = 1$ is still fixed. The next point should be noticed is the variations of $x_1 = 0.5$. Except the variation 3, a dash-dot styled line with $x_{12} = 0.3$, three cases converge to $x^* = 1$. The only difference between these three cases is the infiltrating ratio $x_{1,2}$. Since such infiltrators get

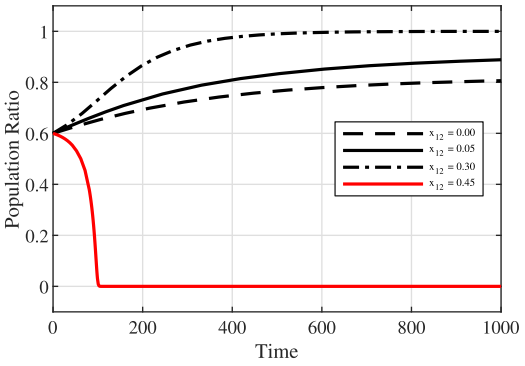

FIGURE 6. Convergence of ***stable coexistence*** with respect to $x_{1,2}$.

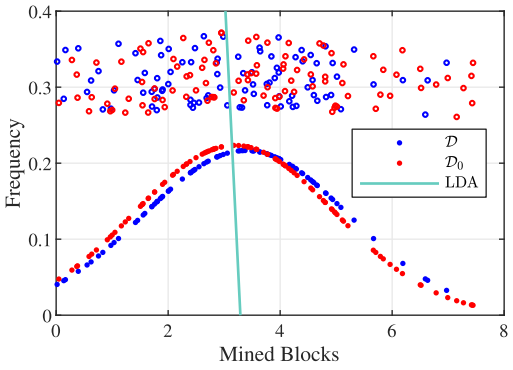

FIGURE 7. Statistical distance on normal approximations $\mathcal{D}$ and $\mathcal{D}_0$.

a mining reward without working honestly and redistribute it to the original pool, the demand at the right level has proved necessary by game theoretic approach [25]. If not, Fig. 5 also implies that the increase in infiltrating ratio to the appropriate level further accelerates the convergence rate, but also shows the convergence totally reversed if $x_{1,2}$ exceeds that level. Indeed, stable coexistence strategy has one more feature about increasing $x_{1,2}$. As shown in Fig. 6, the ESS converges from stable coexistence to dominating strategy up to certain level as the infiltrating ratio increases. These result provide a reasonable reference for assigning infiltrator ratio $x_{i,j}$.

In Fig. 7, we depict the statistical distinguishability on existence of malicious infiltrators among 100 individual miners. On the same parameter setting of Fig. 6 with $x_{1,2} = 0.05$, a solid line, which converges to the interior ESS, we constructed a Poisson samples based on the PoW consensus with an expected number of mined blocks and its frequency for each miners. The corresponding control group is non-attacked pool, and we can approximate two sets with a normal distribution according to the Lemma 1. To check whether individual miner can detect the infiltrators or not, we applied linear discriminant analysis(LDA) that separates two classes of events which is also well-known in pattern recognition or machine learning. The necessity for LDA is the conditional pdf of sample is normally distributed, which fits well with our model. LDA attempts to figure out the best separating line of two classes of data by maximizing the distance between centers while minimizing the variances. In most cases, LDA outputs a line divides both groups into almost half which implies indistinguishability and two distributions $\mathcal{D}$ and $\mathcal{D}_0$ almost overlapped. In short, the effect of infiltrators seems indistinguishable in general, which supports Theorem 2.

Now, we investigate the feasibility of our manipulation discussed at Theorem 3. Main idea is the existence of a boundary point such that the increase in the required block size only induces the *mover* to migrate while the *anchor* still stays in the original pool. For the convenience of visibility, we adjust several parameters as $R_0 = 1500, \tau = 600$, $\rho = 3000$ and $(h_1, h_2) = (2.5, 2)$. For $n = 1000$ miners, we set the mover at 10% of $n_1 = x_1\, n$ and assume the anchor

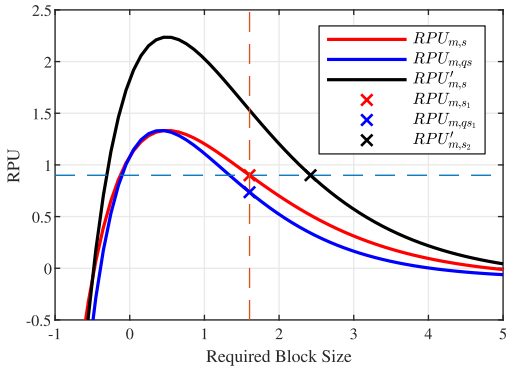

FIGURE 8. RPU of the mover with $(x_1, x_2) = (0.6, 0.4)$.

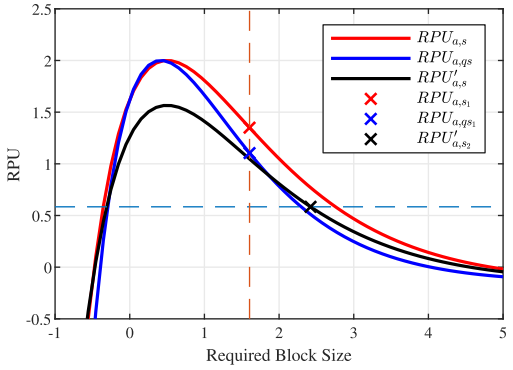

FIGURE 9. RPU of the anchor with $(x_1, x_2) = (0.6, 0.4)$, $k = 1.5$.

yields 1.5 times higher mining power than the mover, i.e., $k = 1.5$. Fig. 8 presents RPU_{m,s_1}, RPU_{m,qs_1} and RPU'_{m,s_2} where $q = 1.2$. As shown in the figure, both RPU_{m,s_1} and RPU_{m,qs_1}, the red and blue lines respectively, have exactly same global maximum RPU but the corresponding required block size became smaller for RPU_{m,qs_1} when $q > 1$. We already discussed at Remark 4 that such block size maximizes the mover's revenue rather than the anchor's is undesirable in the view of mining pool, so we may consider the monotone decreasing part of RPU_{m,s_1} only. Then we may assume that the mover is in a balance between pool 1 and pool 2, that is, $RPU_{m,s_1} = RPU'_{m,s_2}$. Hence, the mover has enough reason to

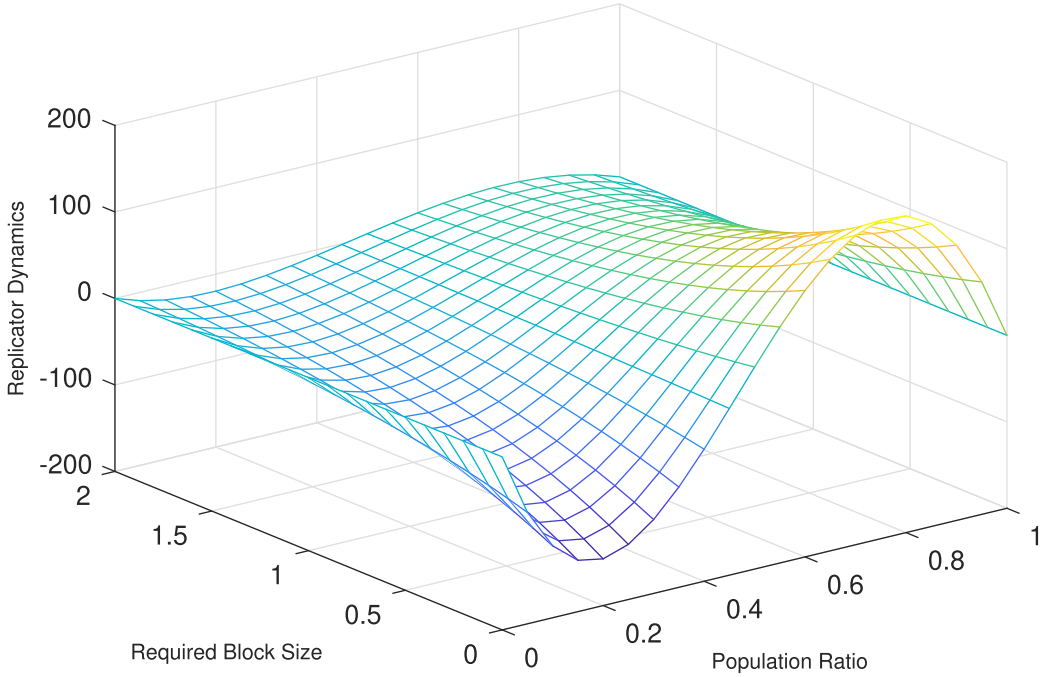

FIGURE 10. Replicator dynamics of the pool selection with respect to the population ratio x_1 and the required block size s_1.

TABLE 3. Concrete parameters for better response learning.

Parameter	Value
Total population size	$n = 1000$
Population fractions	$(x_1, x_2) = (0.6, 0.4)$
Infiltrating rates	$(x_{1,2}, x_{2,1}) = (0.05, 0.03)$
Hash rates	$(h_1, h_2) = (2.5, 2)$
Propagation delay	$\tau = 600$
Average mining time	$T = 600$
Mining reward	$R_0 = 1500$
Transaction fee per unit block size	$r = 3000$
Unit electricity charge per hash rate	$p = 0.1$
Ratio of changed block size	$q = 1.2$
Ratio of yield difference	$k = 1.5$

migrate to pool 2 by the inequality $RPU_{m,qs_1} < RPU'_{m,s_2}$ if pool 1 requires larger block size as qs_1.

On the other hand, the anchor's RPU does not follow the same aspect. With the same block sizes s_1 and s_2 of pool 1 and pool 2 respectively, we always get $RPU_{a,s_1} > RPU_{a,s_2}$ as Fig. 9. Furthermore, still $RPU_{a,qs_1} > RPU'_{a,s_2}$ holds unlike the mover side and the anchor does not willing to migrate. Note that $|\frac{\partial}{\partial s}RPU_{a,qs}| > |\frac{\partial}{\partial s}RPU'_{a,s}|$ for $s \geq s_1$, it is clear that there must be a break-even point for the anchor as $RPU_{a,qs'_1} = RPU'_{a,s'_2}$ and this supports that our inductive step will work properly.

Finally, we present the replicator dynamics as a function of both x_1 and s_1. Note that, the miner's dilemma can be categorized as a prisoner's dilemma, i.e., the destination of block withholding attack cannot yield the maximal total utility for every participated pools and the global maximum of RPU is meaningless. Under this circumstance, the pool need to migrate their own miners by adjusting required block size and Fig. 10 explains it well. For a fixed block size there are exactly 2 critical points, and if x_1 is interposed between the boundary and the closer critical point, the replicator equation enforces the vanishing of that pool. Also Fig. 10 implies the pool with relatively higher population more attempts to migrate their own miners. Moreover, as required block size increases, the replicator dynamics converges to the zero line. That is, enough portion of miners finished to migrate and the remaining anchors are barely willing to move without high stimulation due to their enormous mining power, i.e., the mining game almost reached to the ESS.

VI. CONCLUSION

In this paper, we have investigated the evolutionary mining game with *miner's dilemma* under block withholding attack which affects the population dynamics of mining pool. We have modelled a rigorous game theoretic model to analyze the ESS of replicator dynamics and evolutionary stability of mining pool selection in the view of pools. Based on the statistics, we have designed an approximation for successful mining rate which affected by malicious infiltrators to verify if individual miners will migrate themselves. Moreover, we have constructed a reward scheme that moves the configuration from initial state to a desired ESS by allowing a better response learning. The numerical analysis have demonstrated the feasibility of our approach and provided the guarantee for our theoretical discoveries.

Our study focuses on the detailed process of evolutionarily stable movements. Unlike the static analysis of existing

results, the dynamics is more complicated to analyze at once due to the intervention of time sequences even though it is strongly required to be applied in practice. As our future work, we may consider the extended model for the scenario of multiple pools joined with multiple network-related parameters. We also expect the results obtained in this work to provide a new approach for more sophisticated blockchain network model which can be used to analyze both security and vulnerability, especially block size limit controversy.

REFERENCES

[1] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: http://bitcoin.org/bitcoin.pdf

[2] V. Buterin, "A next-generation smart contract and decentralized application platform," Ethereum, White Paper, 2014. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper

[3] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *Proc. IEEE Symp. Secur. Privacy (SP)*, San Jose, CA, USA, May 2016, pp. 839–858.

[4] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. Kishigami, "Blockchain contract: Securing a blockchain applied to smart contracts," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2016, pp. 467–468.

[5] Y. Zhang and J. Wen, "An IoT electric business model based on the protocol of bitcoin," in *Proc. 18th Int. Conf. Intell. Next Gener. Netw. (ICIN)*, Paris, France, Feb. 2015, pp. 184–191.

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

[7] A. Bahga and V. K. Madisetti, "Blockchain platform for industrial Internet of Things," *J. Softw. Eng. Appl.*, vol. 9, no. 10, pp. 533–546, Oct. 2016.

[8] M. Conoscenti, A. Vetrò, and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review," in *Proc. IEEE/ACS 13th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Agadir, Morocco, Nov./Dec. 2016, pp. 1–6.

[9] 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, 2018.

[10] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the Internet of Things," *IEEE Access*, vol. 6, pp. 32979–33001, 2018.

[11] E. Karafiloski and A. Mishev, "Blockchain solutions for big data challenges: A literature review," in *Proc. IEEE Int. Conf. Smart Technol.*, Ohrid, Macedonia, Jul. 2017, pp. 763–768.

[12] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, and C. Weinhardt, "A blockchain-based smart grid: Towards sustainable local energy markets," *Comput. Sci.-Res. Develop.*, vol. 33, nos. 1–2, pp. 207–214, 2018.

[13] C. Liu, K. K. Chai, X. Zhang, E. T. Lau, and Y. Chen, "Adaptive blockchain-based electric vehicle participation scheme in smart grid platform," *IEEE Access*, vol. 6, pp. 25657–25665, 2018.

[14] M. Mylrea and S. N. G. Gourisetti, "Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security," in *Proc. Resilience Week*, 2017, pp. 18–23.

[15] J. Basden and M. Cottrell, "How utilities are using blockchain to modernize the grid," in *Harvard Business Review Digital Articles*. Brighton, MA, USA: Harvard Business Review, 2017, pp. 2–5.

[16] A. Stanciu, "Blockchain based distributed control system for Edge computing," in *Proc. 21st Int. Conf. Control Syst. Comput. Sci.*, Bucharest, Romania, May 2017, pp. 667–671.

[17] H. Liu, Y. Zhang, and T. Yang, "Blockchain-enabled security in electric vehicles cloud and edge computing," *IEEE Netw.*, vol. 32, no. 3, pp. 78–83, May/Jun. 2018.

[18] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When mobile blockchain meets edge computing," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 33–39, Aug. 2018.

[19] Q. I. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, pp. 14757–14767, 2017.

[20] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain," *J. Med. Syst.*, vol. 42, no. 8, p. 140, 2018.

[21] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in *Proc. 18th Int. Conf. Financial Cryptogr. Data Secur.*, Mar. 2014, pp. 436–454.

[22] G. O. Karame, E. Androulaki, and S. Capkun, "Double-spending fast payments in bitcoin," in *Proc. 19th ACM Conf. Comput. Commun. Secur. (CCS)*, Oct. 2012, pp. 906–917.

[23] M. Rosenfeld, "Analysis of bitcoin pooled mining reward systems," 2011, *arXiv:1112.4980*. [Online]. Available: https://arxiv.org/abs/1112.4980

[24] T. Neudecker and H. Hartenstein. (2019). *Short Paper: An Empirical Analysis of Blockchain Forks in Bitcoin*. [Online]. Available: http://dsn.tm.kit.edu/bitcoin/forks/blockprop.pdf

[25] I. Eyal, "The miner's dilemma," in *Proc. 36th IEEE Symp. Secur. Privacy (SP)*, May 2015, pp. 89–103.

[26] N. T. Courtois and L. Bahack, "On subversive miner strategies and block withholding attack in bitcoin digital currency," 2014, *arXiv:1402.1718*. [Online]. Available: https://arxiv.org/abs/1402.1718

[27] 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. Secur. Found. Symp. (CSF)*, Verona, Italy, Jul. 2015, pp. 397–411.

[28] A. Laska, B. Johnson, and J. Grossklags, "When bitcoin mining pools run dry: A game-theoretic analysis of the long-term impact of attacks between mining pools," in *Proc. 2nd Workshop Bitcoin Res. (BITCOIN)*, Jan. 2015, pp. 63–77.

[29] 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. Commoun. Secur. (CCS)*, Oct. 2017, pp. 195–209.

[30] 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. 6, pp. 760–763, Oct. 2018.

[31] Y. Li, X. Ding, and H. Li, "Robust consensus of networked evolutionary games with attackers and forbidden profiles," *Entropy*, vol. 20, no. 1, p. 15, 2018.

[32] R. Qin, Y. Yuan, and F.-Y. Wang, "Research on the selection strategies of blockchain mining pools," *IEEE Trans. Computat. Social Syst.*, vol. 5, no. 3, pp. 748–757, Sep. 2018.

[33] Y. Wang, C. Tang, F. Lin, Z. Zheng, and Z. Chen, "Pool strategies in PoW-based blockchain networks: Game-theoretic analysis," *IEEE Access*, vol. 7, pp. 8427–8436, 2019.

[34] C. Tang, C. Li, X. Yu, Z. Zheng, and Z. Chen, "Cooperative mining in blockchain networks with zero-determinant strategies," *IEEE Trans. Cybern.*, to be published. doi: 10.1109/TCYB.2019.2915253.

[35] P. Rizun, "A transaction fee market exists without a block size limit," *Block Size Limit Debate Working Paper*, Aug. 2015. [Online]. Available: https://www.bitcoinunlimited.info/resources/feemarket.pdf and http://www.ledgerjournal.org/ojs/index.php/ledger/article/view/96

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

[37] J. Hofbauer and K. Sigmund, "Evolutionary game dynamics," *Bull. Amer. Math. Soc.*, vol. 40, no. 4, pp. 479–519, 2003.

[38] C. Adami and A. Hintze, "Evolutionary instability of zero-determinant strategies demonstrates that winning is not everything," *Nature Commun.*, vol. 4, Aug. 2013, Art. no. 2193.

[39] R. Cressman, *Evolutionary Dynamics and Extensive Form Games*. Cambridge, MA, USA: MIT Press, 2003.

[40] A. Spiegelman, I. Keidar, and M. Tennenholtz, "Game of coins," 2018, *arXiv:1805.08979*. [Online]. Available: https://arxiv.org/abs/1805.08979

[41] B. Biais, C. Bisière, M. Bouvard, and C. Casamatta, "The blockchain folk theorem," *Rev. Financial Stud.*, vol. 32, no. 5, pp. 1662–1715, Apr. 2019. doi: 10.1093/rfs/hhy095.

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

[43] C. Decker and R. Wattenhofer, "Information propagation in the bitcoin network," in *Proc. IEEE 13th Int. Conf. Peer-Peer Comput. (P2P)*, Sep. 2013, pp. 1–10.

[44] G. Andresen. *Back-of-the-Envelope Calculations for Marginal Cost of Transactions*. Accessed: Apr. 4, 2015. [Online]. Available: https://gist.github.com/gavinandresen/5044482

[45] J. Hofbauer, P. Schuster, and K. Sigmund, "A note on evolutionary stable strategies and game dynamics," *J. Theor. Biol.*, vol. 81, no. 3, pp. 609–612, 1979.

SEONGGEUN KIM (S'19) received the B.S. and M.S. degrees from the School of Mathematical Science, Korea Advanced Institute of Science and Technology (KAIST), Daejeon, South Korea, in 2014 and 2016, respectively, where he is currently pursuing the Ph.D. degree with the School of Mathematical Science.

He has contributed several articles to the International Conference on Information Security and Cryptology (ICISC). His research interests include lattice-based post quantum cryptography, functional encryption, information theory, and game theoretic analysis in blockchain. Since 2016, he has been a Student Member with the Korean Mathematical Society, Seoul, South Korea.

SANG-GEUN HAHN (M'18) received the B.S. degree in mathematics from Seoul National University, Seoul, South Korea, in 1979, the M.S. degree in mathematics from the New Mexico Institute of Mining and Technology, Socorro, NM, USA, in 1983, and the Ph.D. degree in mathematics from The Ohio State University, Columbus, OH, USA, in 1987.

He was a Lecturer with The Ohio State University, from 1986 to 1987. In 1989, he was a newly appointed Professor of mathematical sciences with the Korea Advanced Institute of Science and Technology (KAIST) and served as an Adjunct Professor with the Graduate School of Information Security, in 2011. He is the author of one book, more than 30 articles, and holds one patent. His research interests include number theory, lattice and code-based post quantum cryptography, social network analysis on robustness, blockchain, and quantum computing.