# Evolutionary Game for Mining Pool Selection in Blockchain Networks

Xiaojun Liu, Wenbo Wang, *Member, IEEE*, Dusit Niyato, *Fellow, IEEE*,
Narisa Zhao, and Ping Wang, *Senior Member, IEEE*

***Abstract*—In proof-of-work-based blockchain networks, the block miners participate in a crypto-puzzle solving competition to win the reward of publishing (i.e., mining) new blocks. Due to the remarkable difficulty of the crypto-puzzle, individual miners tend to join mining pools to secure stable profits. We study the dynamics of mining pool selection in a blockchain network, where mining pools may choose arbitrary block mining strategies. We identify the hash rate for puzzle-solving and the block propagation delay as two major factors determining the mining competition results. We then model the strategy evolution of individual miners as an evolutionary game. We provide the theoretical analysis of evolutionary stability in the pool selection dynamics for a two-pool case. Numerical simulations support our theoretical findings as well as demonstrate the stability in the evolution of miners' strategies in a general case.**

***Index Terms*—Blockchain, mining pool, evolutionary game.**

## I. Introduction

A PUBLIC blockchain network is built as an overlay peer-to-peer (P2P) network for decentralized temper-proof data recording, trusted timestamping or general-purpose distributed autonomous organization [1]. The Nakamoto consensus protocol [2] is adopted to financially incentivize the full nodes (block miners) to abide by the "longest-chain rule" for blockchain state maintenance. Following the protocol, a block miner packs an arbitrary set of verified transactions into a data structure, known as a candidate "block", and broadcasts it to the entire network. The blockchain state is maintained as a linear list of blocks linked by hash pointers [2] in a loosely synchronized manner. Namely, a miner always keeps the longest observed chain as its local blockchain replica.

The incentive mechanism of the Nakamoto protocol consists of two parts [2]: (a) a computation-intensive crypto-puzzle solving process to make Sybil attacks financially unaffordable, and (b) a reward confirmation process to award an incentive to the miners when their published blocks are recognized by the network. The crypto-puzzle solving process is implemented as a Proof-of-Work (PoW) competition [2], where the miners exhaustively query a trusted random oracle, e.g., a SHA-256 hash function, to find a random string satisfying a preimage condition based on their own block proposals. In the awarding process, the miner which first gets its candidate block disseminated across the network receives a reward in digital tokens for its effort in validating new transactions [1]. Compared with the prevalent incentive mechanisms in mobile networks [3], [4], the Nakamoto protocol is characterized by a decentralized token-issuing scheme embedded in its block-confirmation functionality. With a fixed reward per block, a node's willingness to join the consensus process is mainly influenced by the expected cost of energy consumption.

The probability of winning a PoW competition depends on the ratio between a miner's hash rate, i.e., the number of queries to the hash function that the miner makes per second, and the total hash rate of the entire network [2]. Meanwhile, the block propagation time in the P2P network determines the final result of block confirmation within one consensus round, since only the first block propagated to the majority of the nodes will be accepted as the new head of the blockchain [5], [6]. Practically, the chance for individual miners to win a PoW competition is negligible due to the overwhelming hash rate in the network. As a result, the real-world blockchain networks are dominated by the proxy nodes that represent the coalitions of miners known as mining pools [1]. A mining pool works as a task scheduler by dividing a preimage-searching task into smaller sub-tasks and assigning them to the miners in the pool according to their devoted/reported hash rate. By aggregating the hash rate of many miners, the probability for a mining pool to win a block reward becomes significantly large. Then, an individual miner can secure its small, but stable share of reward according to its share of hash rate in the pool.

In this letter, we study the problem of mining pool selection in a PoW-based blockchain network. We consider that the individual miners are bounded rational and the mining pools adopt arbitrary mining strategies [7]. We model the pool-selection dynamics in the network as an evolutionary game. We focus on the impact of the hash rate and propagation delay on the strategy evolution, and study the evolutionary stability of the pool-selection dynamics in the case of two mining pools.

## II. Problem Formulation

### A. Financially Incentivized Block Mining With Proof-of-Work

We consider a PoW-based blockchain network [2] with $N$ individual miners, which organize themselves into $M$ mining pools, the set of which is denoted by $\mathcal{M} = \{1, 2, \dots, M\}$. We assume that the crypto-puzzle solving

Manuscript received January 8, 2018; revised March 5, 2018; accepted March 22, 2018. Date of publication March 27, 2018; date of current version October 11, 2018. This work was supported in part by the Singapore MOE Tier 1 under Grant 2017-T1-002-007 RG122/17, and in part by the Singapore MOE Tier 2 under Grant MOE2014-T2-2-015 ARC4/15 and Grant NRF2015-NRF-ISF001-2277. The associate editor coordinating the review of this paper and approving it for publication was M. Dong. *(Corresponding author: Xiaojun Liu.)*

X. Liu and N. Zhao are with the Institute of Systems Engineering, Dalian University of Technology, Dalian 116024, China (e-mail: liuxiaojun@mail.dlut.edu.cn; nmgnrs@dlut.edu.cn).

W. Wang, D. Niyato, and P. Wang are with the School of Computer Engineering, Nanyang Technological University, Singapore 639798 (e-mail: wbwang@ntu.edu.sg; dniyato@ntu.edu.sg; wangping@ntu.edu.sg).

Digital Object Identifier 10.1109/LWC.2018.2820009

process is ASIC-resistant [1]. In other words, the miners use general-purpose computing units for hash queries and have roughly the same hashing efficiency, i.e., hash rate per Watt. A mining pool $i$ requires a certain hash rate, $\omega_i$, to be provided by each miner joining the pool. Let $\boldsymbol{\omega} = [\omega_1, \ldots, \omega_M]^\top$ denote the hash rate vector. Further, let $\mathbf{x} = [x_1, \ldots, x_M]^\top$ denote the vector of population fraction for the pools such that $\mathbf{x}$ is in an $(M-1)$-simplex, i.e., $\mathcal{X} = \{\mathbf{x} \in \mathbb{R}_+^M : \sum_{i\in\mathcal{M}} x_i = 1\}$. Then, the probability for pool $i$ to win a mining competition is [1]

$$\Pr_i^{\text{mine}}(\mathbf{x}, \boldsymbol{\omega}) = \frac{\omega_i x_i}{\sum_{j=1}^{M} \omega_j x_j}. \tag{1}$$

Pool $i$ broadcasts a mined block to the peers to propagate it to the entire network. The block propagation time is determined by both the transmission delay over each link and the transaction verification time at each relaying node. For a block of size $s$, the transmission delay can be modeled as $\tau_p(s) = \frac{s}{\gamma c}$, where $\gamma$ is a network scale-related parameter, and $c$ is the average effective channel capacity of each link [5]. Meanwhile, since verifying a transaction requires a fixed amount of computation, the block verification time can be modeled as a linear function $\tau_v(s) = \beta s$, where $\beta$ is a parameter determined by both the network scale and the average verification speed of each node. Then, the average time for a block of size $s$ to be propagated across the network is

$$\tau(s) = \tau_p(s) + \tau_v(s) = \frac{s}{\gamma c} + \beta s. \tag{2}$$

The incidence of abandoning (i.e., orphaning) a valid candidate block due to the propagation delay follows a Poisson process with mean rate $1/T$, which is maintained by the network as a fixed average mining rate [2]. Thereby, the probability of orphaning a valid block of size $s$ is

$$\Pr^{\text{orphan}}(s) = 1 - e^{-\tau(s)/T} = 1 - e^{-(\frac{s}{\gamma c} + \beta s)/T}. \tag{3}$$

Then, the probability for pool $i$ to ultimately win a mining race with a block of size $s_i$ is

$$\Pr_i^{\text{win}}(\mathbf{x}, \boldsymbol{\omega}, s_i) = \frac{\omega_i x_i}{\sum_{j=1}^{M} \omega_j x_j} e^{-(\frac{s_i}{\gamma c} + \beta s_i)/T}. \tag{4}$$

The block reward is comprised of a fixed token-issuing reward and the fees of the transactions packed in the new block [1]. Consider that the blockchain users pay a fixed fee per transaction and the transaction records have the same size. Let $R$ denote the token-issuing reward and $\rho$ denote the transaction confirmation price per unit data size. Then, the transaction fees can be expressed as $\rho s_i$ [6]. The miners also have to consider the energy cost due to hash computation. Let $p$ denote the energy price for maintaining a unit hash rate during $T$. The energy cost can be expressed as $p\omega_i$. Based on (4), a miner's expected payoff in pool $i$ can be expressed as

$$y_i(\mathbf{x}, \boldsymbol{\omega}, s_i) = \frac{R + \rho s_i}{N x_i} \frac{\omega_i x_i}{\sum_{j=1}^{M} \omega_j x_j} e^{-(\frac{s_i}{\gamma c} + \beta s_i)/T} - p\omega_i. \tag{5}$$

### *B. Mining Pool Selection As an Evolutionary Game*

Consider that each individual miner is bounded rational and aims to maximize its payoff given in (5). Then, we can define the evolutionary game for mining pool selection as a 4-tuple: $\mathcal{G} = \langle \mathcal{N}, \mathcal{M}, \mathbf{x}, \{y_i(\mathbf{x}, \boldsymbol{\omega}, s_i)\}_{i\in\mathcal{M}} \rangle$, where (a) $\mathcal{N}$ is the population of individual miners and $|\mathcal{N}| = N$, (b) $\mathcal{M} = \{1, 2, \ldots, M\}$ is the set of mining pools, (c) $\mathbf{x} \in \mathcal{X}$ is the vector of the population states, and (d) $\{y_i(\mathbf{x}, \boldsymbol{\omega}, s_i)\}_{i\in\mathcal{M}}$ is the set of individual miner's payoffs in each mining pool. We note that $\omega_i$ and $s_i$ form the predetermined strategy of pool $i$. Then, by the pairwise proportional imitation protocol [8], the replicator dynamics for the population evolution can be expressed as the following system of Ordinary Differential Equations (ODEs), $\forall i \in \mathcal{M}$ [8]:

$$\dot{x}_i(t) = f_i(\mathbf{x}(t)) = x_i(t)(y_i(\mathbf{x}(t); \boldsymbol{\omega}, s_i) - \bar{y}(\mathbf{x}(t))), \tag{6}$$

where $\dot{x}_i(t)$ is the growth rate of the size of pool $i$ over time, and $\bar{y}(\mathbf{x}) = \sum_{i=1}^{M} y_i(\mathbf{x}; \boldsymbol{\omega}, s_i) x_i$ is the average payoff of the miners in the pools. Let $Y(\mathbf{x}) = [y_1(\mathbf{x}), \ldots, y_M(\mathbf{x})]^\top$ denote the vector of payoffs for all the mining pools. The Nash Equilibria (NE) of $\mathcal{G}$ can be defined as follows:

*Definition 1 (NE [9]):* A population state $\mathbf{x}^* \in \mathcal{X}$ is in a set of NE $\mathcal{E}(Y)$ of game $\mathcal{G}$, i.e., $\mathbf{x}^* \in \mathcal{E}(Y)$, if for all feasible states $\mathbf{x} \in \mathcal{X}$ the inequality $(\mathbf{x} - \mathbf{x}^*)^\top Y(\mathbf{x}^*) \le 0$ holds.

It is straightforward that the NE is a fixed point of the ODEs given in (6), namely, $\forall i \in \mathcal{M}, f_i(\mathbf{x}(t)) = 0$ [8]. Then, we need to further investigate the stability of an NE state $\mathbf{x}^* \in \mathcal{E}(Y)$ for pool selection. Suppose that there exists another population state $\mathbf{x}'$ trying to invade state $\mathbf{x}^*$ by attracting a small share $\epsilon \in (0, 1)$ in the population of miners to switch to $\mathbf{x}'$. Then, $\mathbf{x}^*$ is an Evolutionary Stable Strategy (ESS) if the following condition holds for all $\epsilon \in (0, \bar{\epsilon})$:

$$\sum_{i\in\mathcal{M}} x_i^* y_i((1-\epsilon)\mathbf{x}^* + \epsilon\mathbf{x}') \ge \sum_{i\in\mathcal{M}} x_i' y_i((1-\epsilon)\mathbf{x}^* + \epsilon\mathbf{x}'). \tag{7}$$

Based on (7), we can formally define the ESS as follows.

*Definition 2 (ESS [9]):* A population state $\mathbf{x}^*$ is an ESS of game $\mathcal{G}$, if there exists a neighborhood $\mathcal{B} \in \mathcal{X}$, such that $\forall \mathbf{x} \in \mathcal{B} - \mathbf{x}^*$, the condition $(\mathbf{x} - \mathbf{x}^*)^\top Y(\mathbf{x}^*) = 0$ implies that $(\mathbf{x}^* - \mathbf{x})^\top Y(\mathbf{x}) \ge 0$.

We present in Algorithm 1 the strategy evolution of the $N$ miners following the pairwise proportional imitation protocol [8]. As the population increases, the protocol represents the replicator dynamics described by (6).

**Algorithm 1** Pairwise Proportional Imitation Protocol for Mining Pool Selection

```
Initialization: (a) $\forall i \in \mathcal{N}$, miner $i$ randomly selects a mining
  pool to start with. (b) $t \leftarrow 1$.
while x has not converged and $t <$ MAX_COUNTER do
    for $i \in \mathcal{N}$ do
        $j \leftarrow \mathrm{Rand}(1, M)$ {Randomly selects a pool $j \in \mathcal{M}$}
        Determine whether to switch to pool $j$ according to the
        switching probability $\rho_{i,j}$:
            $\rho_{i,j} = x_j \max(y_j(\mathbf{x}, \boldsymbol{\omega}, s_j) - y_i(\mathbf{x}, \boldsymbol{\omega}, s_i), 0)$    (8)
    end for
    $t \leftarrow t + 1$
end while
```

### C. A Case Study of Two Mining Pools

Due to the space limit, we study the case of two mining pools ($M = 2$) to exemplify the procedure of stability analysis for the NE in the pool-selection game. Let the population fraction of each pool be $x_1 = x$, and $x_2 = 1 - x$. From Definition 1 and by solving $\dot{x}_i(t) = 0, i \in [1, 2]$, we can obtain three rest points of the ODEs given by (6) in the form of $(x^*, 1 - x^*)$:

$$x^* \in \left\{0, 1, \frac{a-b}{Np(\omega_1 - \omega_2)^2} - \frac{\omega_2}{\omega_1 - \omega_2}\right\}, \tag{9}$$

where after some mathematical manipulations we have $a = (R + \rho s_1)\omega_1 e^{-(\frac{s_1}{\gamma c} + \beta s_1)/T}$ and $b = (R + \rho s_2)\omega_2 e^{-(\frac{s_2}{\gamma c} + \beta s_2)/T}$. It is worth noting that $a$ and $b$ represent the expected reward of an individual miner in pool 1 and pool 2, respectively. To fulfill the condition for $\mathbf{x}$ to be in the $(M - 1)$-simplex, we also have $0 < \frac{a-b}{Np(\omega_1-\omega_2)^2} - \frac{\omega_2}{\omega_1-\omega_2} < 1$.

Now, we are ready to investigate the evolutionary stability of the three fixed points. In the cases of $x^* = 0$ and $x^* = 1$, the population states are $(0, 1)$ and $(1, 0)$, respectively. We know that the two fixed points are of the similar form, since the individual payoff functions are similar for each mining pool. Therefore, we only need to check the case with $x_1 = x^* = 0$.

*Lemma 1:* For game $\mathcal{G}$ with two mining pools, 1) The rest point with $x^* = 0$ is an ESS, if

$$\begin{cases} \frac{a-b}{N\omega_2} - p(\omega_1 - \omega_2) < 0, \text{ and} \\ \left(\frac{a-b}{N\omega_2} - p(\omega_1 - \omega_2)\right)\left(p\omega_2 - \frac{b}{N\omega_2}\right) > 0. \end{cases} \tag{10}$$

2) The rest point with $x^* = \frac{a-b}{Np(\omega_1-\omega_2)^2} - \frac{\omega_2}{\omega_1-\omega_2}$ is an ESS if for $c = a - b + Np\omega_2(\omega_2 - \omega_1)$,

$$\begin{cases} \frac{c(a(\omega_1+\omega_2)+\omega_1(-2b+Np\omega_1(\omega_2-\omega_1)))}{(a-b)} < 0, \text{ and} \\ \frac{pc(-b\omega_1+a\omega_2)(a-b+Np\omega_1(\omega_2-\omega_1))}{(\omega_1-\omega_2)} > 0. \end{cases} \tag{11}$$

*Proof:* By [8, Definition 2.6], the asymptotically stable state of the ODEs in (6) is guaranteed to be an ESS. When the replicator dynamics is continuous-time, it is asymptotically stable if the Jacobian matrix of the dynamical system at the equilibrium is negative definite [10]. For the ODEs in (6), the Jacobian matrix of a network with two mining pools is

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

Further, the elements in (12) are derived as follows:

$$\begin{aligned} \frac{\partial f_1(\mathbf{x})}{\partial x_1} &= (1 - 2x_1)\left(\frac{a}{N(\omega_1 x_1 + \omega_2 x_2)} - p\omega_1\right) \\ &\quad - \frac{a\omega_1(x_1 - x_1^2)}{N(\omega_1 x_1 + \omega_2 x_2)^2} - \frac{b\omega_2 x_2^2}{N(\omega_1 x_1 + \omega_2 x_2)^2} + p\omega_2 x_2, \end{aligned} \tag{13}$$

$$\begin{aligned} \frac{\partial f_1(\mathbf{x})}{\partial x_2} &= p\omega_2 x_1 - \frac{a\omega_2(1 - x_1)x_1}{N(\omega_1 x_1 + \omega_2 x_2)^2} + \frac{b\omega_2 x_1 x_2}{N(\omega_1 x_1 + \omega_2 x_2)^2} \\ &\quad - \frac{b x_1}{N(\omega_1 x_1 + \omega_2 x_2)}, \end{aligned} \tag{14}$$

$$\begin{aligned} \frac{\partial f_2(\mathbf{x})}{\partial x_1} &= p\omega_1 x_2 + \frac{a\omega_1 x1 x_2}{N(\omega_1 x_1 + \omega_2 x_2)^2} - \frac{b\omega_1(1 - x_2)x_2}{N(\omega_1 x_1 + \omega_2 x_2)^2} \\ &\quad - \frac{a x_2}{N(\omega_1 x_1 + \omega_2 x_2)}, \end{aligned} \tag{15}$$

$$\begin{aligned} \frac{\partial f_2(\mathbf{x})}{\partial x_2} &= (1 - 2x_2)\left(\frac{b}{N(\omega_1 x_1 + \omega_2 x_2)} - p\omega_2\right) \\ &\quad - \frac{b\omega_2(x_2 - x_2^2)}{N(\omega_1 x_1 + \omega_2 x_2)^2} - \frac{a\omega_1 x_1^2}{N(\omega_1 x_1 + \omega_2 x_2)^2} + p\omega_1 x_1. \end{aligned} \tag{16}$$

Based on (13)-(16), we have

1) After some standard mathematical manipulations, $J$ is negative definite if the determinants of its principal minors at $x^* = 0$ satisfy the following two conditions:

$$\begin{cases} \det(J_{11}) = \frac{\partial f_1(\mathbf{x})}{\partial x_1} = \frac{a-b}{N\omega_2} - p(\omega_1 - \omega_2) < 0, \text{ and} \\ \det(J) = \left(\frac{a-b}{N\omega_2} - p(\omega_1 - \omega_2)\right)(p\omega_2 - \frac{b}{N\omega_2}) > 0. \end{cases} \tag{17}$$

2) Similarly, at $x^* = \frac{a-b}{Np(\omega_1-\omega_2)^2} - \frac{\omega_2}{\omega_1-\omega_2}$, the following two conditions can be obtained for $J$ to be negative definite:

$$\begin{cases} \det(J_{11}) = \frac{c(a(\omega_1+\omega_2)+\omega_1(-2b+Np\omega_1(\omega_2-\omega_1)))}{N(a-b)(\omega_1-\omega_2)^2} < 0, \text{ and} \\ \det(J) = \frac{pc(-b\omega_1+a\omega_2)(a-b+Np\omega_1(\omega_2-\omega_1))}{N(a-b)^2(\omega_1-\omega_2)} > 0. \end{cases} \tag{18}$$

The inequalities in (17) and (18) are exactly the conditions in (10) and (11) given by Lemma 1, respectively. Therefore, the proof to Lemma 1 is completed. ■

In practical scenarios, the blockchain network is composed of a large population of miners. Then, from Lemma 1, we can employ the asymptotic analysis and obtain the following theorem on the evolutionary stability of the rest points.

*Theorem 1:* Assume that the population size $N$ is sufficiently large. Then, neither of the rest points with $x^* \in \{0, 1\}$ is evolutionary stable. The rest point with $x^* = \frac{a-b}{Np(\omega_1-\omega_2)^2} - \frac{\omega_2}{\omega_1-\omega_2}$ is an ESS if the following conditions are satisfied:

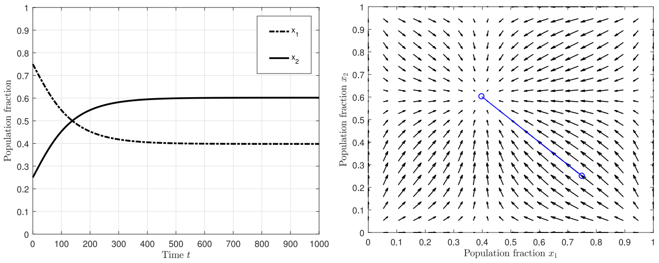
$$\begin{cases} a - b < 0, \text{ and} \\ (b\omega_1 - a\omega_2)(\omega_2 - \omega_1) > 0. \end{cases} \tag{19}$$

*Proof:* At the rest point with $x^* = 0$, by Lemma 1, we can obtain $\lim_{N\to+\infty} \det(J_{11}) \geq 0$ for the Jacobian if $\omega_1 \leq \omega_2$, Then, the Jacobian matrix is not negative definite. Alternatively, if $\omega_1 > \omega_2$, we have $\lim_{N\to+\infty} \det(J_{11}) < 0$ and $\lim_{N\to+\infty} \det(J) < 0$. Again, the Jacobian matrix is also not negative definite. Then, the rest point with $x^* = 0$ is not an ESS. Following the same procedure, we can show that the rest point with $x^* = 1$ is not evolutionary stable either.

Meanwhile, we know that any rest point in the interior of $\mathcal{X}$ is an NE [10]. Then, for the NE with $x^* = \frac{a-b}{Np(\omega_1-\omega_2)^2} - \frac{\omega_2}{\omega_1-\omega_2}$, following Lemma 1, we obtain

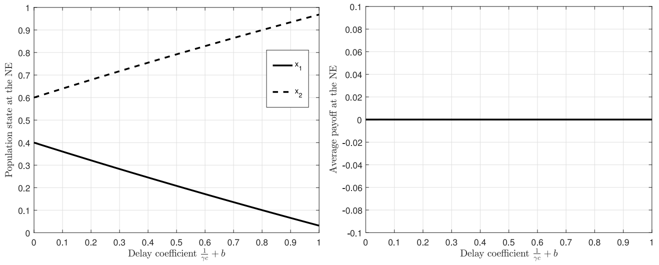
$$\begin{aligned} \lim_{N\to+\infty} \det(J_{11}) &= \lim_{N\to+\infty}\Bigg(\frac{(a - b + Np\omega_2(\omega_2 - \omega_1))a(\omega_1 + \omega_2)}{N(a - b)(\omega_1 - \omega_2)^2} \\ &\quad + \frac{(a - b + Np\omega_2(\omega_2 - \omega_1))\omega_1(-2b + Np\omega_1(\omega_2 - \omega_1))}{N(a - b)(\omega_1 - \omega_2)^2}\Bigg) \\ &= \lim_{N\to+\infty} \frac{Np^2\omega_1\omega_2}{a - b}, \end{aligned} \tag{20}$$

$$\begin{aligned} \lim_{N\to+\infty} \det(J) &= \lim_{N\to+\infty}\Bigg(\frac{p(a - b + Np\omega_2(\omega_2 - \omega_1))}{N(a - b)^2(\omega_1 - \omega_2)} \\ &\quad \times (a\omega_2 - b\omega_1)(a - b + Np\omega_1(\omega_2 - \omega_1))\Bigg) \\ &= \lim_{N\to+\infty} \frac{Np^3\omega_1\omega_2(b\omega_1 - a\omega_2)(\omega_2 - \omega_1)}{(a - b)^2}. \end{aligned} \tag{21}$$



(a) (b)

Fig. 1. (a) Evolution of the miners' population states over time with two mining pools, and (b) replicator dynamics of the pool-selection strategies and the evolution trajectory from $\mathbf{x}(0) = (0.75, 0.25)$.



(a) (b)

Fig. 2. (a) Stable population state vs. different delay coefficient, and (b) average payoff of the miners vs. different delay coefficient.

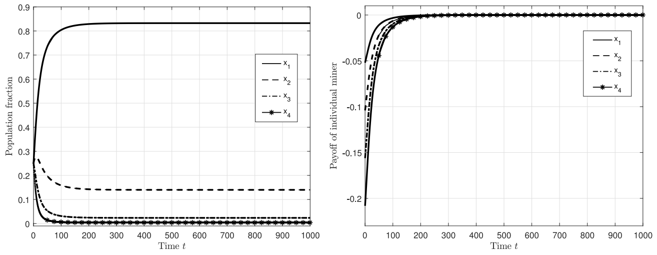
By (20) and (21), the Jacobian matrix is negative definite if the conditions given in (19) are satisfied. Hence the NE $(x^*, 1-x^*)$ is an ESS. Then, the proof to Theorem 1 is completed. ■

## III. Performance Evaluation

In this section, we provide the numerical analysis of the population state evolution in different conditions of the pool-selection game. We first consider a network with $N = 5000$ individual miners, which evolve to form two mining pools (i.e., $M = 2$). We set $\frac{1}{\gamma c} + b = 0.005$, $R = 1000$, $\rho = 2$ and $p = 0.01$. We first set the mining strategy variables of each pool as $s_1 = s_2 = 100$, $\omega_1 = 30$ and $\omega_2 = 20$ such that the conditions in Theorem 1 are satisfied. Figure 1(a) demonstrates the evolution of the population state from an initial point $\mathbf{x}(0) = (0.75, 0.25)$. Figure 1(b) shows that with the given parameter settings, the pool-selection game admits a unique ESS of $\mathbf{x}^* = (0.4, 0.6)$, which is in accordance with our theoretical findings.

With the same network settings, we examine in Figure 2 the evolution of the stable states and the corresponding average payoff at the NE with respect to a different delay coefficient $\frac{1}{\gamma c} + b$. Figure 2(a) shows that as $\frac{1}{\gamma c} + b$ increases, more miners tend to join the pool with a smaller hash rate requirement ($\omega_2 = 20$). Jointly considering the payoffs at the NE (see Figure 2(b)), we know that under the given network settings, a larger delay coefficient leads to a higher probability of orphaning the blocks of the same size. Therefore, the miners prefer to join the pool that induces a lower mining cost.

Finally, we consider in Figure 3 a more general situation with four mining pools, where the pools' mining strategies are set to be $s_i = 100$ $(i \in \{1, \ldots, 4\})$, $\omega_1 = 10$, $\omega_2 = 20$, $\omega_3 = 30$ and $\omega_4 = 40$. We observe from Figure 3(a) that at the NE, selecting the pool with the lowest hash rate requirement (i.e., pool 1) becomes the dominant strategy. Further, Figure 3(b) indicates a situation where the mining process becomes a perfect competition market with an NE payoff of zero, and no miner can switch its pool selection without undermining some other miner's payoff at the equilibrium.



(a) (b)

Fig. 3. (a) Evolution of the population states with four mining pools. (b) Payoffs evolution of the different mining pools.

## IV. Conclusion

In this letter, we have studied the problem of mining pool selection in a blockchain network adopting the proof-of-work scheme. We have modeled the dynamics of pool selection among individual miners as an evolutionary game. We have considered the hash rate and propagation delay to be two major factors that determine the outcome of the block mining competition. Further, we have investigated the evolutionary stability of the pool selection dynamics in the case of two mining pools and revealed the conditions for the network to admit a unique evolutionary stable state. Our numerical evaluation results have provided the numerical evidence for our theoretical discoveries.

## References

[1] 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.

[2] J. Garay, A. Kiayias, and N. Leonardos, "The Bitcoin backbone protocol: Analysis and applications," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.*, Sofia, Bulgaria, Apr. 2015, pp. 281–310.

[3] M. Dong, X. Liu, Z. Qian, A. Liu, and T. Wang, "QoE-ensured price competition model for emerging mobile networks," *IEEE Wireless Commun.*, vol. 22, no. 4, pp. 50–57, Aug. 2015.

[4] X. Liu, M. Dong, K. Ota, P. Hung, and A. Liu, "Service pricing decision in cyber-physical systems: Insights from game theory," *IEEE Trans. Services Comput.*, vol. 9, no. 2, pp. 186–198, Mar./Apr. 2016.

[5] P. R. Rizun, *A Transaction Fee Market Exists Without A Block Size Limit*, Bitcoin Forum, Aug. 2015.

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

[7] B. A. Fisch, R. Pass, and A. Shelat, "Socially optimal mining pools," in *Proc. 13th Int. Conf. Web Internet Econ.*, Bengaluru, India, Dec. 2017, pp. 205–218.

[8] J. W. Weibull, *Evolutionary Game Theory*. Cambridge, MA, USA: MIT Press, 1997.

[9] J. Hofbauer and W. H. Sandholm, "Stable games and their dynamics," *J. Econ. Theory*, vol. 144, no. 4, pp. 1665–1693, 2009.

[10] R. Cressman, *Evolutionary Dynamics and Extensive Form Games*, vol. 5. Cambridge, MA, USA: MIT Press, 2003.