Game-theoretic Approach to Decision-making Problem for Blockchain Mining

Kosuke Toda, Naomi Kuze, Member, IEEE and Toshimitsu Ushio, Member, IEEE

Abstract—It is an important decision-making problem for a miner in blockchain networks if he/she does the mining so that he/she earns a reward by creating a new block earlier than the other miners. We formulate the decision-making problem as a non-cooperative game because the probability of creating blocks depends on not only his/her own computational resource but also other miners’ computational resources. By the theoretical and numerical analysis, we show a hysteresis phenomenon of Nash equilibria depending on the reward and a jump phenomenon of the decision of the miners by a slight change of the reward. We also show that the reward for which miners decide to quit mining becomes smaller as the number of miners increases.

Index Terms—Blockchain, Proof of Work, Decision-making, Game Theory, Hysteresis.

I. INTRODUCTION

Blockchain is distributed ledger technology for recording transactions, and underlies various services such as Bitcoin [1] that is digital currency. In blockchain-based services, transactions are recorded as a chain of blocks by using cryptography. A block consists of a block header and transaction data. A block header contains a cryptographic hash of the previous block, and because of which, the blockchain-based services are resistant to tampering. In these services, users called miners distributedly create blocks, and the longest chain called a main chain is considered to be legitimate. The process of creating blocks is called mining. Proof-of-work (PoW) is a typical consensus algorithm used in blockchain-based services. In this algorithm, the mining difficulty is set, and a block header contains a 4-bit value called nonce. When miners create a block, miners need to find a nonce so that the cryptographic hash value for the previous block satisfies specific conditions (the conditions are determined according to the mining difficulty). In general, a cryptographic hash value for a block is unique according to the nonce contained in the block. Moreover, a nonce that satisfies the specific conditions cannot be calculated directly. Therefore, miners need to make an exhaustive search for finding a nonce that satisfies the conditions, which imposes a lot of computational cost on miners. Consequently, PoW also contributes to the resistance to tampering. When a miner succeeds in creating block and the created block is contained in the main chain, he/she gets a reward.

While blockchain has a lot of advantages such as scalability for the number of users, robustness against failures, and resistance to tampering attacks, the energy consumption for mining is high [2], [3]. Therefore, miners need to consider the balance between energy consumption and the mining reward for deciding whether they join mining or not. There are some studies for resource allocation in blockchain mining considering energy consumption from the perspective of game theory [4]. A non-cooperative game is applied to the analysis of how many computational resources are needed to create a new block [5], [6]. Dimitri [5] discusses how many computational resources are needed for mining under a given cost for computation and shows that the decision on investment for mining depends only on the average cost for mining. Fiat et al. [6] discuss how many computational resources to spend for mining under the upper limit of hash calculation of time unit and show that all miners use all available resources.

In this letter, we consider the case where miners continue calculating hash with paying costs until they create blocks and analyze the relationship between the amount of the mining reward and the decision-making of miners on participation in the mining. We derive the miners’ benefit as a utility function and formulate miners’ decision-making problem as a non-cooperative game. By the theoretical and numerical analysis, we show a hysteresis phenomenon of Nash equilibria depending on the reward and a jump phenomenon of the decisions of the miners by a slight change of the reward. The rest of the letter is organized as follows.

In Section II the decision-making problem is formulated as a non-cooperative game. In Section III we analytically study the Nash equilibria of the game in the case of two miners. In Section IV the numerical analysis is conducted.

II. GAME FORMULATION

A. Miners’ decision making as a game

It is an important decision-making problem for a miner in blockchain networks if he/she does the mining so that he/she earns a reward by creating a new block earlier than the other miners. The probability of success depends on not only his/her own computational resource but also other miners’ computational resources. Thus, the decision-making problem can be formulated as a non-cooperative game where his/her strategy is to do the mining or not to do.

We denote $\mathcal{N} = \{1, 2, \ldots, n\}$ as a set of miners $(n \geq 2)$ in the blockchain network. Each miner $k \in \mathcal{N}$ has a strategy set $S_k = \{0, 1\}$. The strategy $s_k = 1$ denotes that miner $k$ do mining and $s_k = 0$ denotes that miner $k$ quit mining. Let $s = (s_1, \ldots, s_n)$ and $S = \times_{k \in \mathcal{N}} S_k$ be a strategy profile and the set of strategy profiles, respectively. We denote $U : S \rightarrow \mathbb{R}^+$.
as a utility function of all miners and $U_k : S \rightarrow \mathbb{R}$ as a utility function of miner $k \in \mathcal{N}$, i.e., $U(s) = (U_1(s), \ldots, U_n(s))$ for a given strategy profile $s$. Then, the game is described as the following tuple

$$G_n = (\mathcal{N}, S, U).$$

(1)

In Section II-B we will derive the utility function $U_k$.

B. Derivation of utility function

To create a new block, a miner calculates a hash value $H(tx, \text{prev.hash}, \text{nc})$ using the data of the previous block, i.e., the Merkle root of transactions $tx$, the hash of previous block header prev.hash, and the nonce nc. The hash function $H$ outputs an $L$-bit hash value according to inputs ($tx$, prev.hash, and nc). In PoW [1], [7], the miner needs to find a nonce that satisfies

$$H(tx, \text{prev.hash}, \text{nc}) \leq 2^{L-h}. \quad (2)$$

For a given target value $2^{L-h}$ in (2), the probability that a miner creates a block with one hash calculation is

$$P[H(tx, \text{prev.hash}, \text{nc}) \leq 2^{L-h}] = \frac{1}{D},$$

where $D = 2^h$ [8]. The relationship between the blocks and the times when they are created is modeled by a Poisson process [9]. Let $w_k$ be the average number of queries to $H(\cdot)$ of miner $k \in \mathcal{N}$ calculated per unit operating time. The rate $\lambda_k$ of the Poisson process for miner $k$ is given by

$$\lambda_k = \frac{w_k}{D} [10].$$

When the miner $k$ does the mining, he/she needs a cost $c_k \geq 0$ per unit operating time and calculates queries whose average number per unit operating time depend on the cost, that is, we assume that $w_k = f_k(c_k)$, where $f_k : \mathbb{R} \rightarrow \mathbb{R_+}$ is a non-decreasing function. If miner $k$ chooses $s_k = 1$, then the rate of the Poisson process is given by

$$\lambda_k = \frac{s_k f_k(c_k)}{D}.$$

First, we calculate the expected reward for the mining. Let $\mathcal{M} \subseteq \mathcal{N}$ be the set of miners that choose doing mining. We assume that all miners in $\mathcal{M}$ start trying to create a new block at the same time $t = 0$ and they create blocks with the same size. The first miner to create a block that reaches consensus earns a reward $R \geq 1$. Let $B_k(t)$ be the probability of miner $k$’s creating a block earlier than the other miners between $t$ and $t + dt$. Then, using the properties of the Poisson process, we have

$$B_k(t) = \exp(-\lambda_k t) \lambda_k dt \exp(-\lambda_k dt) \prod_{i \in \mathcal{M} \setminus \{k\}} \exp(-\lambda_i (t + dt)) \approx \lambda_k \exp\left(-\sum_{i \in \mathcal{M}} \lambda_i t\right) dt = \lambda_k \exp\left(-\sum_{i \in \mathcal{N}} \lambda_i t\right) dt. \quad (3)$$

From the assumption that all miners create blocks with the same size, the reward $R$ is independent of the miners.

$$P_k(s) = \int_0^\infty \lambda_k \exp\left(-\sum_{i \in \mathcal{N}} \lambda_i t\right) dt = \frac{\lambda_k}{\sum_{i \in \mathcal{N}} \lambda_i} = \frac{s_k f_k(c_k)}{\sum_{i \in \mathcal{N}} s_i f_i(c_i)}.$$

Note that the probability of miner $k$’s earning the reward is 0 when miner $k$ chooses $s_k = 0$. Therefore, for any miner $k \in \mathcal{N}$, the expected reward $R_k(s)$ is

$$R_k(s) = \frac{s_k f_k(c_k)}{\sum_{i \in \mathcal{N}} s_i f_i(c_i)} R. \quad (4)$$

Next, we calculate the expected cost for creating a block. Miners consume a cost to find a nonce. The expected cost $CS_k(s)$ is given by

$$CS_k(s) = c_k \int_0^\infty t \lambda_k \exp\left(-\sum_{i \in \mathcal{N}} \lambda_i t\right) dt = \frac{c_k \lambda_k}{(\sum_{i \in \mathcal{N}} \lambda_i)^2} = \frac{s_k f_k(c_k)}{\sum_{i \in \mathcal{N}} s_i f_i(c_i)} \frac{D_{ck}}{\sum_{i \in \mathcal{N}} s_i f_i(c_i)}. \quad (5)$$

Finally, we define the following utility function $U_k(s)$ as the difference between (4) and (5).

$$U_k(s) = \begin{cases} 0 & \text{if } s = (0, \ldots, 0), \\ \frac{s_k f_k(c_k)}{\sum_{i \in \mathcal{N}} s_i f_i(c_i)} \left(R - \frac{D_{ck}}{\sum_{i \in \mathcal{N}} s_i f_i(c_i)}\right) & \text{otherwise}. \end{cases} \quad (6)$$

Note that, when all miners decide not to do mining, $U_k(s)$ is set 0 for all miners.

C. Extension to mixed strategies

We denote $X = \times_{k \in \mathcal{N}} X_k$ as a mixed strategy space where

$$X_k = \{x_k = (x_k^0, 1 - x_k^0)^T \mid 0 \leq x_k^0 \leq 1\}$$

and $x_k^0$ represents the probability of miner $k$’s choosing $s_k = 0$. Let $x = (x_1, \ldots, x_n)$ and $x-k$ represent a mixed strategy profile of all miners and all other miners except miner $k$, respectively. We denote $e_i^m$ as an $m$-dimensional unit vector in which only the $i$-th component is 1. Note that mixed strategy profiles $(e_1^2, \ldots, e_2^2)$ and $(e_2^3, \ldots, e_3^3)$ correspond to pure strategy profiles $s = (0, \ldots, 0)$ and $s = (1, \ldots, 1)$, respectively. Then, for any mixed strategy profile $x$, the expected utility function $u_k : X \rightarrow \mathbb{R}$ of miner $k \in \mathcal{N}$ is given by

$$u_k(x) = x_k^0 u_k(e_1^2, x_k) + (1 - x_k^0) u_k(e_2^2, x_k).$$

Note that $u_k(e_1^2, x_k)$ and $u_k(e_2^2, x_k)$ are the expected values of the utility when miner $k$ chooses strategy $s_k = 0$ and $s_k = 1$, respectively.
Let $\tilde{\beta}_k : X \to 2^{X_k}$ represent the best response correspondence of miner $k$ for the mixed strategy $x$ as follows.

$$\tilde{\beta}_k(x) = \{x'_k \in X_k | \forall x'_k \in X_k \ u_k(x'_k, x_{-k}) \geq u_k(x'_k, x_{-k})\}.$$  

A mixed strategy $x^*$ satisfying $x^* \in \tilde{\beta}(x^*)$ is called a Nash equilibrium where $\tilde{\beta}(x) = x_k \in N \tilde{\beta}_k(x) \subseteq X$. We denote $\text{NE}(G_n)$ as the set of Nash equilibria in game $G_n$.

### III. THE TWO-MINERS CASE

In this section, we focus on the case where the number of miners is 2, i.e., $\mathcal{N} = \{1, 2\}$ and $f_k(c_k)$ is a linear function, i.e., $f_k(c_k) = v_k c_k$, for all $k \in \mathcal{N}$. The utility functions of two miners in game $G_2$ are written as

$$U_1(s) = \begin{cases} 0 & \text{if } (s_1, s_2) = (0, 0), \\ 0 & \text{if } (s_1, s_2) = (0, 0), \\ \frac{g_s}{s_1 + \epsilon s_2 p_v, p_c} \left( R - \frac{d}{s_1 + \epsilon s_2 p_v, p_c} \right) & \text{otherwise}, \end{cases}$$

$$U_2(s) = \begin{cases} 0 & \text{if } (s_1, s_2) = (0, 0), \\ 0 & \text{if } (s_1, s_2) = (0, 0), \\ \frac{g_s}{s_1 + \epsilon s_2 p_v, p_c} \left( R - \frac{d p_c}{s_1 + \epsilon s_2 p_v, p_c} \right) & \text{otherwise}, \end{cases}$$

where $p_v := v_2/v_1 > 0$, $p_c := c_2/c_1 > 0$, and $d := D/v_1 > 0$. We assume $p_v \geq 1 \ (0 < v_1 \leq v_2)$ without loss of generality.

Strategic forms for finite two-player games are depicted as matrices. Shown in Table I and II are the payoffs for the corresponding strategy profile of miner 1 and 2, respectively. We obtain the set of Nash equilibria in mixed strategies of game $G_2$ as in Proposition I.

**Proposition I:** Assume $p_v \geq 1$. We define the following two functions $g_1 : \mathbb{R} \to \mathbb{R}$ and $g_2 : \mathbb{R} \to \mathbb{R}$.

$$g_1(z) = p_v p_c \left( z - \frac{p_c}{1 + p_v p_c} \right) \left( \frac{2 p_v p_c + 1}{p_v (1 + p_v p_c)} - z \right)^{-1},$$

$$g_2(z) = \left( z - \frac{1}{1 + p_v p_c} \right) \left( \frac{2 p_v p_c}{p_v (1 + p_v p_c)} - z \right)^{-1}.$$  

Let $\alpha_1$ and $\alpha_2$ be $\alpha_1 := g_1(R/d)$ and $\alpha_2 := g_2(R/d)$, respectively. Then, the set $\text{NE}(G_2)$ is given as follows.

If $p_c$ satisfies $p_c \geq 1$, then

$$\text{NE}(G_2) = \begin{cases} \{(e_1, e_2)\} & \text{if } \frac{R}{d} < \frac{p_c}{1 + p_v p_c}, \\ \{(e_1, e_2), (\gamma_1, 1 - \gamma_2)\} & \text{if } \frac{R}{d} = \frac{p_c}{1 + p_v p_c}, \\ \{(e_1^2, e_2), (e_2^2, e_2)\} & \text{if } \frac{R}{d} < \frac{p_c}{1 + p_v p_c}, \\ \{(e_1^2, e_2), (e_2^2, e_2)\} & \text{if } \frac{R}{d} = \frac{p_c}{1 + p_v p_c}, \\ \{(e_2^2, e_2)\} & \text{if } \frac{R}{d} > \frac{p_c}{1 + p_v p_c}, \end{cases}$$

where $\gamma_2 \in (g_2(p_c/(1 + p_v p_c))$ and $\delta_2 \in [g_2(1/p_v), 1]$. If $p_v$ satisfies $1 - 1/p_v \leq p_v < 1$, then

$$\text{NE}(G_2) = \begin{cases} \{(e_1, e_2)\} & \text{if } \frac{R}{d} < \frac{1}{1 + p_v p_c}, \\ \{(e_2, e_2), (\xi_1, 1 - \xi_2)\} & \text{if } \frac{R}{d} = \frac{1}{1 + p_v p_c}, \\ \{(e_1^2, e_2), (e_2^2, e_2)\} & \text{if } \frac{R}{d} < \frac{1}{1 + p_v p_c}, \\ \{(e_1^2, e_2), (e_2^2, e_2)\} & \text{if } \frac{R}{d} = \frac{1}{1 + p_v p_c}, \\ \{(e_2^2, e_2)\} & \text{if } \frac{R}{d} > \frac{1}{1 + p_v p_c}, \end{cases}$$

where $\xi_2 \in [0, 1]$ and $\eta_2 \in [0, 1]$.

**Proof:** Because the pure strategy sets $S_1$ and $S_2$ are finite, there exists at least one Nash equilibrium in game...
From (14), the best response \( G \) of miner 1 changes depending on the range of the value of \( g_{2}(R/d_{i}) \), i.e., we consider the following 5 cases: \( g_{2}(R/d_{i}) < 0 \), \( g_{2}(R/d_{i}) = 0 \), \( 0 < g_{2}(R/d_{i}) < 1 \), \( g_{2}(R/d_{i}) = 1 \), and \( g_{2}(R/d_{i}) > 1 \). Similarly, \( \beta_{2}(x_{j}) \) changes depending on the range of the value of \( g_{1}(R/d_{i}) \).

When \( g_{2}(R/d) \) satisfies \( 0 < g_{2}(R/d) < 1 \), the sign of the right side of (14) changes depending on the value of \( x_{2}^{0} \) as follows.

\[
\begin{align*}
\begin{cases}
    u_{1}(e_{2}^{2}, x_{2}) - u_{1}(e_{1}^{2}, x_{2}) < 0 & \text{if } g_{2}(R/d) < x_{2}^{0} \leq 1, \\
    u_{1}(e_{2}^{2}, x_{2}) - u_{1}(e_{1}^{2}, x_{2}) = 0 & \text{if } x_{2}^{0} = g_{2}(R/d), \\
    u_{1}(e_{2}^{2}, x_{2}) - u_{1}(e_{1}^{2}, x_{2}) > 0 & \text{if } 0 \leq x_{2}^{0} < g_{2}(R/d).
\end{cases}
\end{align*}
\]

Therefore, the best response \( \tilde{\beta}_{1}(x) \) is given by

\[
\tilde{\beta}_{1}(x) = \begin{cases}
\{e_{1}^{2}\} & \text{if } g_{2}^{*}(R/d) < x_{2}^{0} \leq 1, \\
X_{1} & \text{if } x_{2}^{0} = g_{2}^{*}(R/d), \\
\{e_{2}^{2}\} & \text{if } 0 \leq x_{2}^{0} < g_{2}^{*}(R/d).
\end{cases}
\]

Similarly, for the other miner \( \ell \in \mathcal{N} \setminus \{k\} \), we obtain the best response \( \tilde{\beta}_{\ell}(x) \) depending on the range of the value of \( g_{\ell}(R/d) \).

- When \( g_{\ell}(R/d) < 0 \),
  \( \tilde{\beta}_{\ell}(x) = \{e_{2}^{2}\} \).

- When \( g_{\ell}(R/d) = 0 \),
  \( \tilde{\beta}_{\ell}(x) = \begin{cases}
X_{\ell} & \text{if } x_{\ell}^{0} = 0, \\
\{e_{2}^{2}\} & \text{if } 0 < x_{\ell}^{0} \leq 1.
\end{cases} \)

- When \( 0 < g_{\ell}(R/d) < 1 \),
  \( \tilde{\beta}_{\ell}(x) = \begin{cases}
\{e_{1}^{2}\} & \text{if } g_{\ell}(R/d) < x_{\ell}^{0} \leq 1, \\
X_{\ell} & \text{if } x_{\ell}^{0} = g_{\ell}(R/d), \\
\{e_{2}^{2}\} & \text{if } 0 \leq x_{\ell}^{0} < g_{\ell}(R/d).
\end{cases} \)

We derive the set of Nash equilibria in the case of (1). Then, we have the following 9 cases depending on the value range of \( R/d \).

- When \( g_{1}(R/d) = 1 \),
  \( \tilde{\beta}_{1}(x) = \begin{cases}
X_{k} & \text{if } x_{1}^{0} = 1, \\
\{e_{2}^{2}\} & \text{if } 0 \leq x_{1}^{0} < 1.
\end{cases} \)

- When \( g_{2}(R/d) > 1 \),
  \( \tilde{\beta}_{2}(x) = \{e_{2}^{2}\} \).

We derive the range of \( R/d \) satisfying \( 0 < g_{k}(R/d) < 1 \), \( k = 1, 2 \). From (9) and (10), it is easily shown that \( g_{1} \) and \( g_{2} \) are monotonically increasing functions. Therefore, we obtain

\[
\begin{align*}
0 < g_{1}(R/d) < 1 & \Rightarrow \frac{p_{c}}{1 + p_{c}p_{e}} < \frac{R}{d} < \frac{1}{p_{e}}, \\
0 < g_{2}(R/d) < 1 & \Rightarrow \frac{1}{1 + p_{c}p_{e}} < \frac{R}{d} < 1.
\end{align*}
\]

Under the assumption of \( p_{c} \geq 1 \), the magnitude relationship among \( p_{c}/(1 + p_{c}p_{e}), 1/p_{e}, 1/(1 + p_{c}p_{e}) \), and 1 depends on the value of \( p_{c} \) as follows.

1) When \( p_{c} \geq 1 \),
\[
\frac{1}{1 + p_{c}p_{e}} < \frac{p_{c}}{1 + p_{c}p_{e}} < \frac{1}{p_{e}} < 1.
\]

2) When \( 1 - 1/p_{e} \leq p_{c} < 1 \),
\[
\frac{p_{c}}{1 + p_{c}p_{e}} < \frac{1}{1 + p_{c}p_{e}} \leq \frac{1}{p_{e}} < 1.
\]

3) When \( 0 < p_{c} < 1 - 1/p_{e} \),
\[
\frac{p_{c}}{1 + p_{c}p_{e}} < \frac{1}{p_{e}} < 1.
\]

We derive the set of Nash equilibria in the case of (1). Then, we have the following 9 cases depending on the value range of \( R/d \).
The pure strategy profile $s$ line (left figure) and the red line (right figure) represent respectively fixed. Let us consider the case where $\epsilon$ (13), respectively. NE $1$ by the second equation in (11) if boundary of the region (b) and (c), (c) and (d), and (d) and (a) are given $(p_1, p_2)$, respectively. Shown in Fig. 1 is the $p_c - R/d$ parameter plane where $p_v \geq 1$ is fixed.

![Fig. 1. The $p_c - R/d$ parameter plane where $p_v \geq 1$ is fixed.](image1)

When $R/d = 1$, we have $\alpha_1 > 1$ and $\alpha_2 = 1$. From (19) and (20), we have the Nash equilibrium $x^* = (e_2^2, e_2^2)$. When $R/d > 1$, we have $\alpha_1 > 1$ and $\alpha_2 > 1$. From (20), we have the Nash equilibrium $x^* = (e_2^2, e_2^2)$. Therefore, (11) is the set of Nash equilibria. Similarly, we can prove (12) and (13).

For a given $p_v$, the change of the Nash equilibria depending on the value of $R/d$ is affected by the value of $p_c$. Shown in Fig. 1 is the $p_c - R/d$ parameter plane where $p_v \geq 1$ is fixed. If the pair $(p_v, R/d)$ is in the region (a), (b), (c), and (d), the set NE$(G_2)$ satisfies $\text{NE}(G_2) = \{(e_2^2, e_2^2)\}$, $\text{NE}(G_2) = \{(e_2^2, e_2^2), (\alpha_1, 1 - \alpha_1)^T, (\alpha_2, 1 - \alpha_2)^T\}$, $\text{NE}(G_2) = \{(e_2^2, e_2^2)\}$, and $\text{NE}(G_2) = \{(e_2^2, e_2^2)\}$, respectively.

Shown in Figs. 2–4 are the relationship between the value $R/d$ and the value $x_k^0$ ($k = 1, 2$) in Nash equilibria. The blue line (left figure) and the red line (right figure) represent the value $x_k^0$ and $x_k^0$, respectively.

Shown in Fig. 2 is the case where $p_c > 1 - 1/p_v$ is fixed. Let us consider the case where $1 - 1/p_v < p_c < 1$. The pure strategy profile $s = (0, 0)$ is a Nash equilibrium if the value $R/d$ is smaller than $1/p_v$. If the value $R/d$ is larger than $1/p_v$, the pure Nash equilibrium $s = (0, 0)$ disappears and only the pure strategy profile $s = (1, 1)$ is a Nash equilibrium.

The pure strategy profile $s = (1, 1)$ is a Nash equilibrium if the value $R/d$ is larger than $1/(1 + p_v p_c)$. If the value $R/d$ is smaller than $1/(1 + p_v p_c)$, the pure Nash equilibrium $s = (1, 1)$ disappears and only the pure strategy profile $s = (0, 0)$ is a Nash equilibrium.

This change in the Nash equilibria due to the change in $R/d$ implies that, when the mining reward is larger than some value, all the miners make decisions to do mining, and once every miner makes a decision to do mining, they continue to do mining for a while even if the reward decreases to the boundary of the region (b), that is, a hysteresis phenomenon exists in the region. Moreover, a jump phenomenon of the choice of strategy profiles chosen by miners occurs due to the disappearance of Nash equilibria when the reward changes across the boundary of the region.

Shown in Fig. 3 is the case where $p_c = 1 - 1/p_v$. The transition from region (c) to (a), i.e., the jump from one pure strategy profile to another one is observed when the value $R/d$ is equal to $1/p_v = 1/(1 + p_v p_c)$.

![Fig. 3. The case when $(p_v, p_c) = (2, 0.5)$.](image3)

Shown in Fig. 4 is the case where $p_c = 1 - 1/p_v$. The pure strategy profile $s = (0, 1)$ is a Nash equilibria if the value $R/d$ is in $1/p_v < R/d < 1/(1 + p_v p_c)$. Two pure Nash equilibria do not coexist in the interior of each region while mixed strategy profile $(e_2^2, (\zeta_2, 1 - \zeta_2)^T)$ and $(\eta_1, 1 - \eta_1)^T, e_2^2$) are Nash equilibria on its boundary $R/d = 1/p_v$ and $R/d = 1/(1 + p_v p_c)$.
the case where $c \in \mathbb{N}$ and $f_k(c) = vc, v > 0$ for all $k \in \mathbb{N}$. From (6) and these assumptions, $U_k(s)$ is rewritten as

$$U_k(s) = \left\{ \begin{array}{ll}
0 & \text{if } s = (0, \ldots, 0), \\
\left( \frac{R}{\sum_{i \in \mathbb{N}^k} s_i} - \frac{d}{\sum_{i \in \mathbb{N}^k} s_i} \right) & \text{otherwise,}
\end{array} \right.$$ 

where $d := D/v$. The value $d$ is fixed 100 and set $R \in \{0, 1, \ldots, 150\}$. We calculate Nash equilibria for each $R$ when the number of miners $n$ is 2, 3, 4, 5, and 6.

Shown in Fig. 5 is the relationship between the value $R/d$ and the value $x_k^0$ in Nash equilibria for each the number of miners $n$. This result shows that both the hysteresis phenomena and the jump phenomenon of the strategy profiles can be observed regardless of the number of miners when all miners pay the same cost and calculate the same number of hash queries per unit operating time. In addition to above, it implies that, as the number of miners increases, the value $R/d$ of the appearance of a Nash equilibrium $s = (1, \ldots, 1)$ decreases.

Shown in Fig. 6 is the relationship between the number of miners and the $R/d$ value when the Nash equilibrium $s = (1, \ldots, 1)$ appears. This figure shows that the value $R/d$ when the equilibrium $s = (1, \ldots, 1)$ appears is inversely proportional to the number of miners $n$.

This result shows that once the miners decide to do mining, they continue to participate in the mining for smaller rewards as their number increases. Thus, it is very important in the design of blockchain networks to set an initial reward as large as possible to have an incentive to participate in the blockchain networks as a miner. Then, as the number of the participating miners is larger, the reward can be decreased to a smaller amount with keeping their number.

V. Conclusion

We modeled the decision-making problem for the participation in the mining as a non-cooperative game and showed that hysteresis phenomena due to the coexistence of two pure Nash equilibria and jump phenomena of the choice of strategy profiles can be observed depending on the change of the mining reward. Moreover, by numerical calculation, we show that the miners keep participating in the mining for smaller rewards as their number becomes larger. It is future work to analyze Nash equilibria theoretically in the case where the number of miners is more than 2.

REFERENCES

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” http://bitcoin.org/bitcoin.pdf, 2008.
[2] J. Truby, “Decarbonizing Bitcoin: Law and policy choices for reducing the energy consumption of Blockchain technologies and digital currencies,” Energy Research & Social Science, vol. 44, pp. 399–410, 2018.
[3] https://www.cbeci.org/
[4] Z. Liu, N. C. Luong, W. Wang, D. Niyato, P. Wang, Y. C. Liang, and D. I. Kim, “A survey on blockchain: A game theoretical perspective,” IEEE Access, vol. 7, pp. 47615–47643, 2019.
[5] N. Dimitri, “Bitcoin mining as a contest,” Ledger, vol. 2, pp. 31–37, 2017.
[6] A. Fiat, A. Karp, E. Koutsoupias, and C. Papadimitriou, “Energy equilibria in proof-of-work mining,” In Proceedings of the 2019 ACM Conference on Economics and Computation, pp. 489–502, 2019.
[7] J. Debus, “Consensus methods in blockchain systems,” Frankfurt School of Finance & Management, Blockchain Center, Tech. Rep, 2017.
[8] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, “A survey on consensus mechanisms and mining strategy management in blockchain networks,” IEEE Access, vol. 7, pp. 22328–22370, 2019.
[9] N. Houy, “The bitcoin mining game,” Ledger, vol. 1, pp. 53–68, 2016.
[10] D. Kraft, “Difficulty control for blockchain-based consensus systems,” Peer-to-Peer Networking and Applications, vol. 9, no. 2, pp. 397–413, 2016.
[11] D. Fudenberg and J. Tirole, “Game theory,” MIT press, 1991.
[12] R. D. McKelvey, A. M. McLennan, and T. L. Turocy, “Gambit: Software tools for game theory,” Version 15.1.1, http://www.gambit-project.org, 2014.