

# Stability analysis and control of decision-making of miners in blockchain

Kosuke Toda<sup>1</sup>, Naomi Kuze<sup>1</sup>, and Toshimitsu Ushio<sup>1</sup>

<sup>1</sup>Graduate School of Engineering Science, Osaka University, Machikaneyama 1-3, Toyonaka-shi, Osaka, 560–8531, Japan.

## Abstract

To maintain blockchain-based services with ensuring its security, it is an important issue how to decide a mining reward so that the number of miners participating in the mining increases. We propose a dynamical model of decision-making for miners using an evolutionary game approach and analyze the stability of equilibrium points of the proposed model. The proposed model is described by the 1st-order differential equation. So, it is simple but its theoretical analysis gives an insight into the characteristics of the decision-making. Through the analysis of the equilibrium points, we show the transcritical bifurcations and hysteresis phenomena of the equilibrium points. We also design a controller that determines the mining reward based on the number of participating miners to stabilize the state where all miners participate in the mining. Numerical simulation shows that there is a trade-off in the choice of the design parameters.

**Keywords**— B lockchain, Proof-of-work, Decision-making, Evolutionary Game, Bifurcation, Hysteresis, Feedback control.

## 1 Introduction

Blockchain is a distributed ledger technology for recording transactions that underlies various fields such as digital currency like Bitcoin [1], data sharing [2], and computer security [3]. Blockchain-based services use cryptography to record transactions as a chain of blocks. A block consists of a block header and transaction data. The block header contains a cryptographic hash of its previous block, which makes blockchain-based services resistant to tampering. In these services, participants called *miners* create blocks in a distributed manner, and the longest chain of blocks is considered to be legitimate. When a miner succeeds in creating a block, he/she gets a reward called a *mining reward*.

Blockchain-based services approve transactions through a consensus algorithm. As a consensus algorithm, proof-of-work (PoW) is typically used. In this algorithm, the mining difficulty is set using a scalar value called a *nonce* in the block header. To create a block, miners must find a nonce such that the

cryptographic hash value for the previous block satisfies specific conditions. The process of creating blocks is called a *mining*. 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. As a result, an exhaustive search imposes a large computational cost on miners, which contributes to the resistance to tampering. Because transaction approvals depend on miner calculations (such calculations are very costly and require a lot of energy [4, 5]), the participation of many miners is needed to maintain blockchain-based services and ensure blockchain system security [6, 7]. Therefore, it is important to analyze the decision-making problem of whether miners participate in the mining according to the energy consumption and mining rewards.

Game theory is used to analyze interactions among rational decision-makers. Many studies have adopted game theory to analyze blockchain-related issues with PoW [8], such as decision-making problems in the mining considering the energy consumption [9, 10]. Evolutionary game theory has been used as a powerful mathematical tool for analyzing dynamical models of evolutionary selection [11]. Dynamical characteristics of the selection process are modeled by *replicator dynamics*. Control methods for the replicator dynamics have been studied in [12, 13, 14]. Evolutionary game models and replicator dynamics are also used in analyzing blockchain-related issues such as mining pool selection problems [15, 16], and attack scenarios [17].

We previously focused on a decision-making problem of whether miners participate in the mining according to the energy consumption and the mining rewards, and modeled it as a non-cooperative game. Through theoretical and numerical analysis, we showed the property of Nash equilibria [18]. However, in this study, we assumed that, once miners choose a strategy (i.e., participation in the mining or not), they do not change their strategies. Practically, the miners may decide to participate in the mining dynamically based on their current earned mining rewards. It is important to analyze such a dynamical decision-making process.

In this paper, we propose a dynamical model of the decision-making problem for miners, by applying an evo-

lutionary game approach. We analyze the stability of its equilibrium points and show the existence of transcritical bifurcations and hysteresis phenomena with the coexistence of two asymptotically stable equilibrium points: one corresponds to the state where all miners participate in the mining and the other to the state where the number of participating miners is minimum. The former equilibrium point is preferable to maintain blockchain-based services. We propose a controller that determines the mining reward based on the number of current participating miners so as to stabilize the equilibrium point if at least one miner participates in the initial time.

The remainder of this paper is organized as follows. In Section 2, we propose an evolutionary game-based dynamical model of the decision-making process. In Section 3, we analyze the stability of its equilibrium point. In Section 4, we design a state feedback controller to let all miners participate in the mining.

## 2 Dynamical model of decision-making

We assume that miners in a blockchain network are partitioned into two sets  $\mathcal{M}$  and  $\mathcal{N}$ , where miners in  $\mathcal{M}$  always participate in the mining and those in  $\mathcal{N}$  have two strategies, participating in the mining (strategy  $s_k = 1$ ) and not participating in the mining (strategy  $s_k = 0$ ), where  $k \in \mathcal{N}$ . Note that  $\mathcal{M} \cap \mathcal{N} = \emptyset$ . Denoted by  $m$  and  $n$  are the cardinalities of  $\mathcal{M}$  and  $\mathcal{N}$ , respectively (we assume  $m \geq 1$  and  $n \geq 1$ ). We define  $x_0$  and  $x_1$  as the ratios of miners in  $\mathcal{N}$  that choose strategies 0 and 1, respectively. Note that

$$x_0 + x_1 = 1. \quad (2.1)$$

Miners need to find a nonce such that the first  $h$  bits of the hash of the block are all 0. Then,  $D = 2^h$  is the difficulty parameter and  $1/D$  is the probability that a miner creates a block with one hash calculation [19]. When miner  $k \in \mathcal{M} \cup \mathcal{N}$  participates in the mining, he/she needs a cost  $c$  per unit operating time. The average number  $w_k = f_k(c)$  of hash queries calculated per unit operating time by miner  $k$  depends on the cost  $c$ , and we assume that  $f_k(c)$  is the same for all miners. In this paper, for simplicity, we assume  $f_k(c) = vc$  ( $v > 0$ ) for any  $k \in \mathcal{M} \cup \mathcal{N}$ .

The mining of blocks can be described as a Poisson process [20, 21]. That is, the block creation time is exponentially distributed [22]. The rate  $\lambda_k$  of the Poisson process of miner  $k \in \mathcal{M} \cup \mathcal{N}$  is given by  $\lambda_k = w_k/D$  [21]<sup>1</sup>. If miner  $k$  chooses  $s_k = 1$ , then the rate of the Poisson process is  $\lambda_k = s_k f_k(c)/D = s_k c/d$  (we define  $d = D/v$ , in this paper). Let  $R$  be the mining reward. Based on the

previous work [18], the expected reward  $R_k$  and the expected cost  $CS_k$  for the mining of miner  $k$  are calculated as follows.

$$R_k = \frac{\lambda_k}{\sum_{i \in \mathcal{M} \cup \mathcal{N}} \lambda_i} R = \frac{R s_k}{m + n x_1}, \quad (2.2)$$

$$CS_k = \frac{c \lambda_k}{(\sum_{i \in \mathcal{M} \cup \mathcal{N}} \lambda_i)^2} = \frac{d s_k}{(m + n x_1)^2}. \quad (2.3)$$

We define the utility function  $u_i(x_0, x_1)$  of miners that choose the strategy  $i \in \{0, 1\}$  as

$$u_i(x_0, x_1) = \begin{cases} 0 & \text{if } i = 0, \\ \frac{1}{m + n x_1} \left( R - \frac{d}{m + n x_1} \right) & \text{if } i = 1, \end{cases} \quad (2.4)$$

which means that the utility of a miner who participates in the mining is the difference between the expected reward  $R_k$  and the expected cost  $CS_k$ . Based on the principle of the evolutionary game [11], the dynamics of the ratio of miners that choose the strategy  $i$  is given by

$$\frac{\dot{x}_i}{x_i} = u_i(x_0, x_1) - \bar{u}(x_0, x_1) \quad (i = 0, 1), \quad (2.5)$$

where  $\bar{u}(x_0, x_1) = \sum_{i=0}^1 x_i u_i(x_0, x_1)$  is the average utility of all miners. According to (2.4), (2.5) is rewritten as

$$\dot{x}_1 = -\dot{x}_0 = \frac{x_1(1 - x_1)}{m + n x_1} \left( R - \frac{d}{m + n x_1} \right) =: \varphi_R(x_1). \quad (2.6)$$

Thus, the dynamics of the decision-making of miners is described by the above 1st-order differential equation and the reward  $R$  plays an important role in the decision-making of the miners for the participation in the mining. In the following, we investigate stability and stabilization of equilibrium points of (2.6). For that purpose, the concept of a *basin of attraction* [23] is important. Let  $\xi(t; x_1^{\text{init}})$  be the solution of (2.6) that starts from an initial state  $x_1^{\text{init}}$  at time  $t = 0$ . For a given asymptotically stable equilibrium point  $x_1^*$  of (2.6), the basin of attraction is defined as the set of all initial states  $x_1^{\text{init}}$  such that  $\xi(t; x_1^{\text{init}})$  is defined for all  $t \geq 0$  and  $\lim_{t \rightarrow \infty} \xi(t; x_1^{\text{init}}) = x_1^*$ .

## 3 Stability analysis

In this section, we investigate the stability of the equilibrium point  $x_1 = 0, 1, x_1^*$  of (2.6), where

$$x_1^* = \frac{1}{n} \left( \frac{d}{R} - m \right). \quad (3.1)$$

When  $1/(m+n) < R/d < 1/m$ , the equilibrium point  $x_1^*$  satisfies  $0 < x_1^* < 1$ . This equilibrium point is the state where the utility  $u_1(1 - x_1^*, x_1^*)$  is equal to 0, that is, the utility for the strategy 0 is equal to that for the strategy 1.

<sup>1</sup>Note that a combination of independent Poisson processes is still a Poisson process. Thus, the rate of the Poisson process of all miners is written as  $\sum_{i \in \mathcal{M} \cup \mathcal{N}} \lambda_i$ .

Table 1: The relation between  $R/d$  and the stability of equilibrium points.

Condition for $R/d$	$x_1 = 0$	$x_1 = 1$	$x_1 = x_1^*$
$R/d < 1/(m+n)$	S	U	S
$1/(m+n) < R/d < 1/m$	S	S	U
$R/d > 1/m$	U	S	S

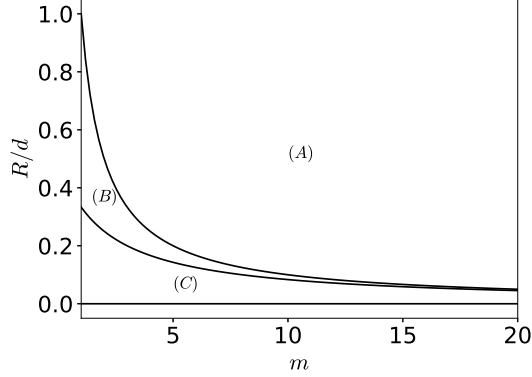


Figure 1: The  $m - R/d$  parameter plane where  $n$  is fixed to  $n = 2$ .

We investigate the local stability of the three equilibrium points. The derivative of  $\varphi_R(x_1)$  with respect to  $x_1$  is

$$\begin{aligned} \frac{\partial \varphi_R(x_1)}{\partial x_1} = & \left( -\frac{x_1}{m+nx_1} + \frac{1-x_1}{m+nx_1} - \frac{nx_1(1-x_1)}{(m+nx_1)^2} \right) \\ & \times \left( R - \frac{d}{m+nx_1} \right) + \frac{dnx_1(1-x_1)}{(m+nx_1)^3}. \end{aligned} \quad (3.2)$$

Thus, we obtain

$$\left. \frac{\partial \varphi_R(x_1)}{\partial x_1} \right|_{x_1=0} = \frac{1}{m} \left( R - \frac{d}{m} \right), \quad (3.3)$$

$$\left. \frac{\partial \varphi_R(x_1)}{\partial x_1} \right|_{x_1=1} = -\frac{1}{m+n} \left( R - \frac{d}{m+n} \right), \quad (3.4)$$

$$\left. \frac{\partial \varphi_R(x_1)}{\partial x_1} \right|_{x_1=x_1^*} = \frac{R^3}{nd^2} \left( \frac{d}{R} - m \right) \left( (m+n) - \frac{d}{R} \right). \quad (3.5)$$

Thus, we have their stability conditions as shown in Table 1, where S (*resp.* U) represents an asymptotically stable (*resp.* unstable) point.

Fig. 1 shows the  $m - R/d$  parameter plane with  $n = 2$  where the meaning of each region is as follows. In the region (A), both  $x_1 = 1$  and  $x_1^* < 0$  are asymptotically stable equilibrium points, and the basin of attraction of  $x_1 = 1$  is  $(0, \infty)$ , that is, every solution of (2.6) starting in  $(0, 1]$  converges to 1. In the region (B), both  $x_1 = 0$  and  $x_1 = 1$  are asymptotically stable equilibrium points, and basins of attraction of  $x_1 = 0$  and  $x_1 = 1$  are

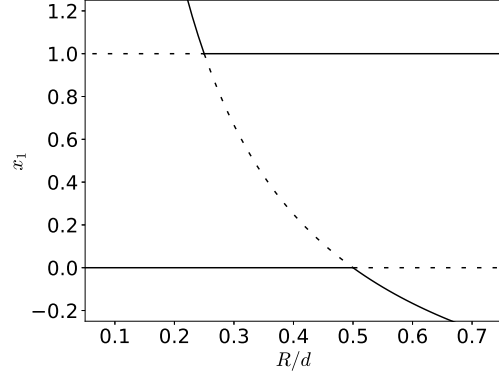


Figure 2: The relation between  $R/d$  and the stability of equilibrium points when  $m = n = 2$ .

$(-\infty, x_1^*)$  and  $(x_1^*, \infty)$ , respectively, that is, every solution of (2.6) starting in  $[0, x_1^*)$  converges to 0, and every solution of (2.6) starting in  $(x_1^*, 1]$  converges to 1. In the region (C), both  $x_1 = 0$  and  $x_1^* > 0$  are asymptotically stable equilibrium points, and the basin of attraction of  $x_1 = 0$  is  $(-\infty, 1)$ , that is, every solution of (2.6) starting in  $[0, 1)$  converges to 0.

Shown in Fig. 2 is a bifurcation diagram with respect to the bifurcation parameter  $R/d$ , where  $m = n = 2$ . The solid (*resp.* dashed) line represents an asymptotically stable (*resp.* unstable) equilibrium point. Two curves of equilibrium points pass through  $(x_1, R) = (1, d/(m+n))$  (*resp.*  $(x_1, R) = (0, d/m)$ ), one given by  $x_1 = x_1^*$ , the other by  $x_1 = 1$  (*resp.*  $x_1 = 0$ ). Both curves exist on both sides of  $R = d/(m+n)$  (*resp.*  $R = d/m$ ). The stability along each curve exchanges on passing through  $R = d/(m+n)$  (*resp.*  $R = d/m$ ). Thus, the exchange of stability (known as a *transcritical bifurcation*) [24] is observed when  $(x_1, R) = (0, d/m), (1, d/(m+n))$ . We show in A that the vector field (2.6) satisfies the condition of the transcritical bifurcation shown in [24].

Since the values of  $x_i$  ( $i = 0, 1$ ) satisfy  $0 \leq x_i \leq 1$ , we observe jump phenomena owing to these transcritical bifurcations. Moreover,  $R > d/m$  needs to be satisfied so that all miners in  $\mathcal{N}$  participate in the mining. It is noted that, once the miners participate in the mining, they continue to participate in the mining until the reward  $R$  becomes  $d/(m+n)$ . Thus, a hysteresis phenomenon of the equilibrium points is observed.

Fig. 3 shows trajectories of (2.6) from an initial state  $x_1^{\text{init}} = 0.1$  (blue) and  $x_1^{\text{init}} = 0.9$  (red). When  $d/(m+n) < R < d/m$ , both  $x_1 = 0$  and  $x_1 = 1$  are asymptotically stable points whose basins of attraction are  $(-\infty, x_1^*)$  and  $(x_1^*, \infty)$ , respectively. Thus, the number of miners who participate in the mining converges to 0 if the initial ratio is less than  $x_1^*$  because their utility is negative and they prefer non-participation.

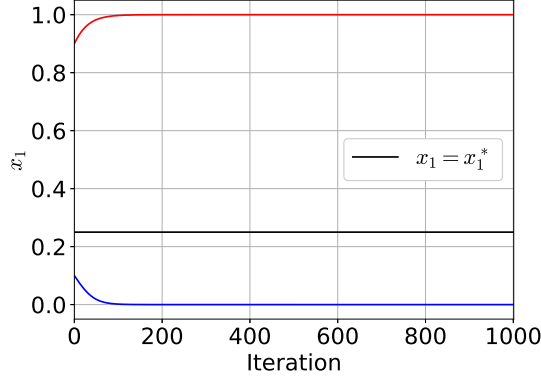


Figure 3: Trajectories of (2.6) when  $m = n = 2$ ,  $d = 100$ , and  $R = 40$ , from  $x_1^{\text{init}} = 0.1$  (blue) and  $x_1^{\text{init}} = 0.9$  (red).

## 4 Stabilization

The result in Section 3 implies that no miner in  $\mathcal{N}$  participates in the mining in the steady state when the mining reward  $R^*$  satisfies  $R^* < d/(m+n)$ . When the mining reward  $R^*$  satisfies  $d/(m+n) < R^* < d/m$ , miners' behaviors depend on the initial state  $x_1^{\text{init}}$ , i.e., no miner in  $\mathcal{N}$  participates in the mining in the steady state when  $x_1^{\text{init}} < x_1^*$ . We propose a state feedback controller to adjust the reward based on the ratio  $x_1$  so that all miners in  $\mathcal{N}$  participate in the mining, i.e., let every trajectory of  $x_1$  with its initial state in  $(0, 1]$  converge to 1.

### 4.1 Case where $R^* < d/(m+n)$

First, we show that  $x_1 = 1$  cannot be stabilized when  $R^* < d/(m+n)$ . We consider the following state feedback controller  $R_1(x_1)$  that adjusts the reward based on the ratio  $x_1$ .

$$R = R_1(x_1), \quad R_1(1) = R^* < \frac{d}{m+n}. \quad (4.1)$$

The controlled trajectory of  $x_1$  by (4.1) is described by

$$\dot{x}_1 = \frac{x_1(1-x_1)}{m+nx_1} \left( R_1(x_1) - \frac{d}{m+n} \right) =: \psi_R(x_1). \quad (4.2)$$

The derivative of  $\psi_R(x_1)$  with respect to  $x_1$  is

$$\begin{aligned} \frac{\partial \psi_R(x_1)}{\partial x_1} &= \left( -\frac{x_1}{m+nx_1} + \frac{1-x_1}{m+nx_1} - \frac{nx_1(1-x_1)}{(m+nx_1)^2} \right) \\ &\quad \times \left( R_1(x_1) - \frac{d}{m+nx_1} \right) \\ &\quad + \frac{x_1(1-x_1)}{m+nx_1} \left( \frac{\partial R_1(x_1)}{\partial x_1} + \frac{dn}{(m+nx_1)^2} \right). \end{aligned} \quad (4.3)$$

We obtain

$$\left. \frac{\partial \psi_R(x_1)}{\partial x_1} \right|_{x_1=1} = -\frac{1}{m+n} \left( R_1(1) - \frac{d}{m+n} \right) > 0. \quad (4.4)$$

Therefore, the unstable equilibrium point  $x_1 = 1$  cannot be stabilized even if the feedback controller is used.

### 4.2 Case where $d/(m+n) < R^* < d/m$

Next, we show that  $x_1 = 1$  can be an asymptotically stable equilibrium point whose basin of attraction is  $(0, 1]$  with a state feedback controller. We introduce the following state feedback controller  $R_2(x_1)$  to adjust the reward based on the ratio  $x_1$ ,

$$R = R_2(x_1) = R^* + \Delta R(x_1), \quad \Delta R(1) = 0, \quad (4.5)$$

and let every trajectory of  $x_1$  with its initial state in  $(0, 1]$  converge to 1.

#### 4.2.1 The condition of the feedback gain

We give  $\bar{x}_1$  satisfying  $x_1^* < \bar{x}_1 \leq 1$  and  $\varepsilon > 0$ . For a given reward  $R^* \in (d/(m+n), d/m)$ , let  $\Delta R(x_1)$  be

$$\Delta R(x_1) = \begin{cases} K(\bar{x}_1 - x_1) & \text{if } x_1 < x_1^* + \varepsilon, \\ 0 & \text{otherwise,} \end{cases} \quad (4.6)$$

where  $K > 0$  is a feedback gain. We obtain a condition for the gain  $K$  and  $\varepsilon$  such that every trajectory of  $x_1$  with its initial state in  $(0, 1]$  converges to 1 as in Proposition 1.

**Proposition 1.** Assume  $d/(m+n) < R^* < d/m$ . Let  $\zeta_R(x_1)$  be

$$\begin{aligned} \zeta_R(x_1) &:= -Kn x_1^2 + (Kn \bar{x}_1 - Km + R^* n) x_1 \\ &\quad + (R^* m + Km \bar{x}_1 - d), \end{aligned} \quad (4.7)$$

and let  $\alpha, \beta$  ( $\alpha < \beta$ ) be real solutions of the quadratic equation  $\zeta_R(x_1) = 0$ . Then, every trajectory of  $x_1$  with its initial state in  $(0, 1]$  converges to 1 if the gain  $K$  and  $\varepsilon$  satisfy

$$K > \frac{d - R^* m}{m \bar{x}_1} (> 0), \quad (4.8)$$

$$0 < \varepsilon \begin{cases} < \beta - x_1^* & \text{if } \beta < 1, \\ \leq 1 - x_1^* & \text{if } \beta \geq 1. \end{cases} \quad (4.9)$$

*Proof.* With the controller (4.5) and (4.6), the dynamics of  $x_1$  ( $x_1 < x_1^* + \varepsilon$ ) is given by

$$\dot{x}_1 = \eta_R(x_1), \quad (4.10)$$

$$\eta_R(x_1) := \frac{x_1(1-x_1)}{m+nx_1} \left( R^* + K(\bar{x}_1 - x_1) - \frac{d}{m+nx_1} \right). \quad (4.11)$$

According to (4.7),  $\eta_R(x_1)$  can be rewritten as

$$\eta_R(x_1) = \frac{x_1(1-x_1)\zeta_R(x_1)}{(m+nx_1)^2}. \quad (4.12)$$

First, we prove that the quadratic equation  $\zeta_R(x_1) = 0$  has two distinct real solutions under (4.8). We have

$$\zeta_R(x_1^*) = K(\bar{x}_1 - x_1^*)(m + nx_1) > 0, \quad (4.13)$$

which implies with (4.8) that the quadratic equation  $\zeta_R(x_1) = 0$  has two distinct real solutions  $\alpha, \beta$  satisfying  $\alpha < x_1^* < \beta$ .

Next, we prove  $\alpha < 0$  under (4.8). We obtain

$$\begin{aligned} \zeta_R(0) &= m\bar{x}_1K - (d - R^*m) \\ &> m\bar{x}_1 \frac{d - R^*m}{m\bar{x}_1} - (d - R^*m) = 0, \end{aligned} \quad (4.14)$$

from (4.7) and (4.8). Since  $\zeta_R(x_1)$  is a convex upward quadratic function, the smaller solution  $\alpha$  of  $\zeta_R(x_1) = 0$  satisfies  $\alpha < 0$ .

Finally, we prove that the system controlled by (4.5) satisfies  $\dot{x}_1 > 0$  for any  $x_1 \in (0, 1)$  under (4.8) and (4.9). When  $\beta < 1$ ,  $\eta_R(x_1) > 0$  for any  $x_1 \in (0, \beta)$  from (4.12). It is obvious that  $\dot{x}_1 > 0$  for any  $x_1 \in (0, x_1^* + \varepsilon)$  from (4.9). For any  $x_1 \in [x_1^* + \varepsilon, 1)$ ,  $\dot{x}_1 > 0$  because  $K = 0$ . Thus,

$$\dot{x}_1 > 0 \text{ for any } x_1 \in (0, 1). \quad (4.15)$$

Similary, it is also shown by (4.9) that (4.15) holds for any  $\beta \geq 1$ . Therefore, every trajectory of  $x_1$  with its initial state in  $(0, 1]$  converges to 1 under (4.8) and (4.9).  $\square$

It is noted that  $\bar{x}_1 < \beta$  since  $d/(m+n) < R^*$ . So, (4.6) is continuous if  $\varepsilon = \bar{x}_1 - x_1^*$ .

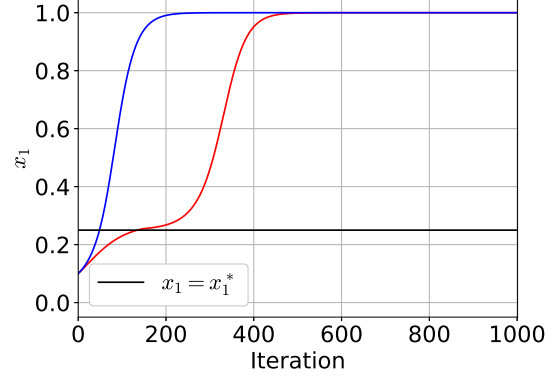
#### 4.2.2 Performance evaluation

In this section, we provide the numerical analysis of the controller. We consider the case where  $m = n = 2$ ,  $d = 100$ , and  $R^* = 40$ . Then, we have  $x_1^* = 0.25$  from (3.1). Let the initial state of  $x_1$  be  $x_1^{\text{init}} = 0.1$ . We consider the following two cases where  $K$  and  $\varepsilon$  satisfy (4.8) and (4.9).

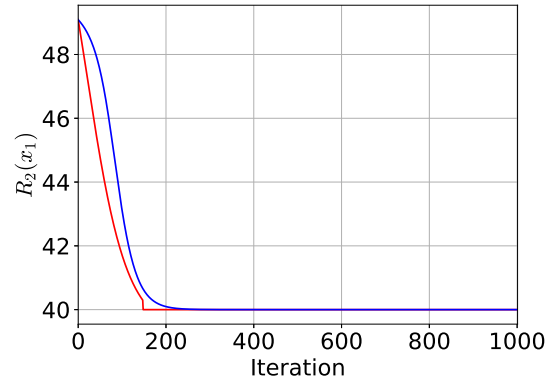
**Case 1)**  $\bar{x}_1 = 0.26$ ,  $\varepsilon = 0.005$ ,  $K = 56.8125$ .

**Case 2)**  $\bar{x}_1 = 1$ ,  $\varepsilon = 0.75$ ,  $K = 10.1$ .

Fig. 4 shows trajectories of the state and the reward. The red and blue lines represent the trajectories of Cases 1) and 2), respectively. In Case 1), it takes a longer time than Case 2) for the state  $x_1$  to converge to 1, but the reward  $R_2(x_1)$  returns to the original value  $R^*$  quickly. Note that  $R_2(x_1)$  in Case 1) is not continuous because we switch the input  $\Delta R(x_1)$  to 0 when  $x_1 = x_1^* + \varepsilon$  (see (4.6)). In Case 2), the state  $x_1$  converges to 1 quickly, but it takes longer time than Case 1) for the reward  $R_2(x_1)$  to return to its original value  $R^*$ . Thus, there is a trade-off in the choice of the design parameters  $\bar{x}_1$  and  $\varepsilon$ .



(a)



(b)

Figure 4: Trajectories of (a) the state  $x_1$  and (b) the reward  $R_2(x_1)$  with a feedback controller satisfying Proposition 1, when  $m = n = 2$ ,  $d = 100$ ,  $R^* = 40$ ,  $x_1^* = 0.25$  from  $x_1^{\text{init}} = 0.1$ , where  $\bar{x}_1 = 0.26, \varepsilon = 0.005, K = 56.8125$  (red) and  $\bar{x}_1 = 1, \varepsilon = 0.75, K = 10.1$  (blue).

## 5 Conclusion

We proposed a dynamical model of the decision-making of miners in the blockchain. The proposed model is described by the 1st-order differential equation. So, it is simple but its theoretical analysis gives an insight into the characteristics of the decision-making. We analyzed the stability of its equilibrium points. We showed the occurrence of the transcritical bifurcations and observed a hysteresis phenomenon. We also proposed a feedback controller and showed that it can stabilize the state where all miners participate in the mining from any non-zero initial participation ratio of the miners. Our future work is to extend our model to the case where miners' computational performances are different from each other.

## Acknowledgements

This research was supported by JST ERATO JPM-JER1603.

## A Transcritical bifurcation

We consider the following system.

$$\dot{x} = f(x, \mu), \quad x \in \mathbb{R}, \quad \mu \in \mathbb{R}. \quad (\text{A.1})$$

We assume that

$$f(x, \mu) = xF(x, \mu), \quad (\text{A.2})$$

where  $F : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$  satisfies the following condition.

$$F(x, \mu) := \begin{cases} \frac{f(x, \mu)}{x} & x \neq 0, \\ \frac{\partial f(0, \mu)}{\partial x} & x = 0. \end{cases} \quad (\text{A.3})$$

Then, it is shown in [24] that (A.1) undergoes a transcritical bifurcation at  $(x, \mu) = (0, 0)$  if the following three conditions hold.

$$(\text{T1}) \quad f(0, 0) = 0, \quad \frac{\partial f(0, 0)}{\partial x} = 0,$$

$$(\text{T2}) \quad \frac{\partial f(0, 0)}{\partial \mu} = 0,$$

$$(\text{T3}) \quad \frac{\partial^2 f(0, 0)}{\partial x \partial \mu} \neq 0, \quad \frac{\partial^2 f(0, 0)}{\partial x^2} \neq 0.$$

Thus we will show that (2.6) satisfies the above three conditions at  $(x_1, R) = (0, d/m), (1, d/(m+n))$ .

### A.1 Case where $(x_1, R) = (0, d/m)$

First, we consider the following coordination transformation by which  $(x_1, R) = (0, d/m)$  is transformed to  $(x, \mu) = (0, 0)$ .

$$\begin{pmatrix} x_1 \\ R \end{pmatrix} = \begin{pmatrix} x \\ \mu \end{pmatrix} + \begin{pmatrix} 0 \\ \frac{d}{m} \end{pmatrix}. \quad (\text{A.4})$$

Then, we define

$$\begin{aligned} f(x, \mu) &:= \varphi_{\mu + \frac{d}{m}}(x) \\ &= \frac{x(1-x)}{m+nx} \left( \mu + \frac{d}{m} - \frac{d}{m+nx} \right) = xF(x, \mu), \end{aligned} \quad (\text{A.5})$$

where the function  $F$  is defined by

$$F(x, \mu) := \frac{1-x}{m+nx} \left( \mu + \frac{d}{m} - \frac{d}{m+nx} \right). \quad (\text{A.6})$$

Then, we have

$$\begin{aligned} \frac{\partial f(x, \mu)}{\partial x} &= F(x, \mu) + x \frac{\partial F(x, \mu)}{\partial x} \\ &= \left( -\frac{x}{m+nx} + \frac{1-x}{m+nx} - \frac{nx(1-x)}{(m+nx)^2} \right) \\ &\quad \times \left( \mu + \frac{d}{m} - \frac{d}{m+nx} \right) + \frac{dnx(1-x)}{(m+nx)^3}. \end{aligned} \quad (\text{A.7})$$

It is obvious that

$$F(x, \mu) = \frac{f(x, \mu)}{x} \quad (\text{A.8})$$

when  $x \neq 0$  and

$$F(0, \mu) = \frac{\mu}{m} = \frac{\partial f(0, \mu)}{\partial x} \quad (\because (\text{A.7})) \quad (\text{A.9})$$

when  $x = 0$ . Thus, the function  $f$  defined by (A.5) satisfies (A.2) and (A.3).

Next, we show that  $f(x, \mu)$  satisfies the conditions (T1) – (T3). We obtain

$$\frac{\partial f(x, \mu)}{\partial \mu} = \frac{x(1-x)}{m+nx}, \quad (\text{A.10})$$

$$\frac{\partial^2 f(x, \mu)}{\partial x \partial \mu} = -\frac{x}{m+nx} + \frac{1-x}{m+nx} - \frac{nx(1-x)}{(m+nx)^2}, \quad (\text{A.11})$$

$$\begin{aligned} \frac{\partial^2 f(x, \mu)}{\partial x^2} &= \left( \frac{n^2 x(1-x)}{(m+nx)^2} - \frac{n(1-x)}{m+nx} + \frac{nx}{m+nx} - 1 \right) \\ &\quad \times \frac{2}{m+nx} \left( \mu + \frac{d}{m} - \frac{d}{m+nx} \right) + \frac{2dn}{(m+nx)^3} \\ &\quad \times \left( \frac{-2nx(1-x)}{m+nx} - x + (1-x) \right). \end{aligned} \quad (\text{A.12})$$

Thus,  $f(x, \mu)$  satisfies the conditions (T1) – (T3) because

$$f(0, 0) = 0, \quad (\text{A.13})$$

$$\frac{\partial f(0, 0)}{\partial x} = 0, \quad (\text{A.14})$$

$$\frac{\partial f(0, 0)}{\partial \mu} = 0, \quad (\text{A.15})$$

$$\frac{\partial^2 f(0, 0)}{\partial x \partial \mu} = \frac{1}{m} \neq 0, \quad (\text{A.16})$$

$$\frac{\partial^2 f(0, 0)}{\partial x^2} = \frac{2dn}{m^3} \neq 0. \quad (\text{A.17})$$

### A.2 Case where $(x_1, R) = (1, d/(m+n))$

It is noted that the dynamics of  $x_0$  is written as follows.

$$\begin{aligned} \dot{x}_0 &= -\frac{x_0(1-x_0)}{m+n(1-x_0)} \left( R - \frac{d}{m+n(1-x_0)} \right) \\ &= -\varphi_R(1-x_0) \end{aligned} \quad (\text{A.18})$$

because  $x_0$  and  $x_1$  satisfies (2.1). Thus, it is sufficient to show that (A.18) undergoes a transcritical bifurcation at  $(x_0, R) = (0, d/(m+n))$ . We consider the following coordination transformation by which  $(x_0, R) = (0, d/(m+n))$  is transformed to  $(x, \mu) = (0, 0)$ .

$$\begin{pmatrix} x_0 \\ R \end{pmatrix} = \begin{pmatrix} x \\ \mu \end{pmatrix} + \begin{pmatrix} 0 \\ \frac{d}{m+n} \end{pmatrix}. \quad (\text{A.19})$$

Then, we define

$$\begin{aligned}
f(x, \mu) &:= -\varphi_{\mu + \frac{d}{m+n}}(1-x) \\
&= -\frac{x(1-x)}{m+n(1-x)} \\
&\quad \times \left( \mu + \frac{d}{m+n} - \frac{d}{m+n(1-x)} \right) \\
&= xF(x, \mu), \tag{A.20}
\end{aligned}$$

where the function  $F$  is defined by

$$\begin{aligned}
F(x, \mu) &:= -\frac{1-x}{m+n(1-x)} \\
&\quad \times \left( \mu + \frac{d}{m+n} - \frac{d}{m+n(1-x)} \right). \tag{A.21}
\end{aligned}$$

Then, we have

$$\begin{aligned}
\frac{\partial f(x, \mu)}{\partial x} &= -\left( \frac{-x + (1-x)}{m+n(1-x)} + \frac{nx(1-x)}{(m+n(1-x))^2} \right) \\
&\quad \times \left( \mu + \frac{d}{m+n} - \frac{d}{m+n(1-x)} \right) \\
&\quad + \frac{dnx(1-x)}{(m+n(1-x))^3}. \tag{A.22}
\end{aligned}$$

It is obvious that

$$F(x, \mu) = \frac{f(x, \mu)}{x} \tag{A.23}$$

when  $x \neq 0$  and

$$F(0, \mu) = -\frac{\mu}{m+n} = \frac{\partial f(0, \mu)}{\partial x} \quad (\because \text{A.22}) \tag{A.24}$$

when  $x = 0$ . Thus, the function  $f$  defined by (A.20) satisfies (A.2) and (A.3).

In the same way as Appendix A.1, we obtain the partial derivatives of  $f(x, \mu)$  and show that  $f(x, \mu)$  defined by (A.18) satisfies the conditions (T1) – (T3) because

$$f(0, 0) = 0, \tag{A.25}$$

$$\frac{\partial f(0, 0)}{\partial x} = 0, \tag{A.26}$$

$$\frac{\partial f(0, 0)}{\partial \mu} = 0, \tag{A.27}$$

$$\frac{\partial^2 f(0, 0)}{\partial x \partial \mu} = -\frac{1}{m+n} \neq 0, \tag{A.28}$$

$$\frac{\partial^2 f(0, 0)}{\partial x^2} = \frac{2dn}{(m+n)^3} \neq 0. \tag{A.29}$$

Therefore, (2.6) undergoes transcritical bifurcations at  $(x_1, R) = (0, d/m), (1, d/(m+n))$ .

## References

- [1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008. [Online]. Available: <http://bitcoin.org/bitcoin.pdf>
- [2] Q. 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. 14 757–14 767, 2017.
- [3] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, “Fairaccess: a new blockchain-based access control framework for the internet of things,” *Security and Communication Networks*, vol. 9, no. 18, pp. 5943–5964, 2016.
- [4] 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.
- [5] “Cambridge bitcoin electricity consumption index,” (accessed on 1 March 2021). [Online]. Available: <https://www.cbeci.org/>
- [6] W. Cai, Z. Wang, J. B. Ernst, Z. Hong, C. Feng, and V. C. M. Leung, “Decentralized applications: The blockchain-empowered software system,” *IEEE Access*, vol. 6, pp. 53 019–53 033, 2018.
- [7] Y. Liu, Z. Fang, M. H. Cheung, W. Cai, and J. Huang, “A social welfare maximization mechanism for blockchain storage,” *arXiv preprint arXiv:2103.05866*, 2021.
- [8] Z. Liu, N. C. Luong, W. Wang, D. Niyato, P. Wang, Y. Liang, and D. I. Kim, “A survey on blockchain: A game theoretical perspective,” *IEEE Access*, vol. 7, pp. 47 615–47 643, 2019.
- [9] N. Dimitri, “Bitcoin mining as a contest,” *Ledger*, vol. 2, pp. 31–37, 2017.
- [10] A. Fiat, A. Karlin, E. Koutsoupias, and C. Papadimitriou, “Energy equilibria in proof-of-work mining,” in *Proceedings of the 2019 ACM Conference on Economics and Computation*, 2019, pp. 489–502.
- [11] J. W. Weibull, *Evolutionary game theory*. MIT press, 1997.
- [12] T. Kanazawa, H. Goto, and T. Ushio, “Replicator dynamics with dynamic payoff reallocation based on the government’s payoff,” *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E91-A, no. 9, pp. 2411–2418, 2008.

- [13] T. Kanazawa, Y. Fukumoto, T. Ushio, and T. Misaka, "Replicator dynamics with pigovian subsidy and capitation tax," *Nonlinear Analysis, Theory, Methods and Applications*, vol. 71, no. 12, pp. e818–e826, 2009.
- [14] T. Morimoto, T. Kanazawa, and T. Ushio, "Subsidy-based control of heterogeneous multiagent systems modeled by replicator dynamics," *IEEE Transactions on Automatic Control*, vol. 61, no. 10, pp. 3158–3163, 2016.
- [15] X. Liu, W. Wang, D. Niyato, N. Zhao, and P. Wang, "Evolutionary game for mining pool selection in blockchain networks," *IEEE Wireless Communications Letters*, vol. 7, no. 5, pp. 760–763, 2018.
- [16] K. Fujita, Y. Zhang, M. Sasabe, and S. Kasahara, "Mining pool selection problem in the presence of block withholding attack," in *Proceedings of 2020 IEEE International Conference on Blockchain*, 2020, pp. 321–326.
- [17] S. Kim and S. G. Hahn, "Mining pool manipulation in blockchain network over evolutionary block withholding attack," *IEEE Access*, vol. 7, pp. 144 230–144 244, 2019.
- [18] K. Toda, N. Kuze, and T. Ushio, "Game-theoretic approach to a decision-making problem for blockchain mining," *IEEE Control Systems Letters*, vol. 5, no. 5, pp. 1783–1788, 2021.
- [19] J. Debus, "Consensus methods in blockchain systems," *FSBC Working Paper*, 2017. [Online]. Available: <http://www.fs-blockchain.de/>
- [20] N. Houy, "The bitcoin mining game," *Ledger*, vol. 1, pp. 53–68, 2016.
- [21] D. Kraft, "Difficulty control for blockchain-based consensus systems," *Peer-to-Peer Networking and Applications*, vol. 9, no. 2, pp. 397–413, 2016.
- [22] S. Kasahara and J. Kawahara, "Effect of bitcoin fee on transaction-confirmation process," *Journal of Industrial & Management Optimization*, vol. 15, no. 1, pp. 365–386, 2019.
- [23] H. K. Khalil, *Nonlinear systems*, 3rd ed. Prentice Hall, 2002.
- [24] S. Wiggins, *Introduction to applied nonlinear dynamical systems and chaos*, 2nd ed. Springer, 2003.