Bitcoin vs. Bitcoin Cash: Coexistence or Downfall of Bitcoin Cash?

Yujin Kwon*, Hyoungshick Kim†, Jinwoo Shin*, Yongdae Kim*
*KAIST
{dbwls8724, jinwoos, yongdaek}@kaist.ac.kr
†Sungkyunkwan University
hyoung@skku.edu

***Abstract*—Bitcoin has become the most popular cryptocurrency based on a peer-to-peer network. In Aug. 2017, Bitcoin was split into the original Bitcoin (BTC) and Bitcoin Cash (BCH). Since then, miners have had a choice between BTC and BCH mining because they have compatible proof-of-work algorithms. Therefore, they can freely choose which coin to mine for higher profit, where the profitability depends on both the coin price and mining difficulty. Some miners can immediately switch the coin to mine only when mining difficulty changes because the difficulty changes are more predictable than that for the coin price, and we call this behavior *fickle mining*.**

In this paper, we study the effects of fickle mining by modeling a game between two coins. To do this, we consider both fickle miners and some *factions* (e.g., BITMAIN for BCH mining) that stick to mining one coin to maintain that chain. In this model, we show that fickle mining leads to a Nash equilibrium in which only a faction sticking to its coin mining remains as a loyal miner to the less valued coin (e.g., BCH), where loyal miners refer to those who conduct mining even after coin mining difficulty increases. This situation would cause severe centralization, weakening the security of the coin system.

To determine which equilibrium the competing coin systems (e.g., BTC vs. BCH) are moving toward, we traced the historical changes of mining power for BTC and BCH and found that BCH often lacked loyal miners until Nov. 13, 2017, when the difficulty adjustment algorithm of BCH mining was changed. However, the change in difficulty adjustment algorithm of BCH mining led to a state close to the stable coexistence of BTC and BCH. We also demonstrate that the lack of BCH loyal miners may still be reached when a fraction of miners automatically and repeatedly switches to the most profitable coin to mine (i.e., automatic mining). According to our analysis, as of Dec. 2018, loyal miners to BCH would leave if more than about 5% of the total mining capacity for BTC and BCH has engaged in the automatic mining. In addition, we analyze the recent "hash war" between Bitcoin ABC and SV, which confirms our theoretical analysis. Finally, we note that our results can be applied to any competing cryptocurrency systems in which the same hardware (e.g., ASICs or GPUs) can be used for mining. Therefore, our study brings new and important angles in competitive coin markets: a coin can *intentionally* weaken the security and decentralization level of the other rival coin when mining hardware is shared between them, allowing for automatic mining.

I. Introduction

Bitcoin [1] is the most popular cryptocurrency based on a distributed and public digital ledger called *blockchain*. Nodes in the Bitcoin network store the blockchain, where transactions are recorded in a unit of a *block*, and the blockchain is extended by generating new blocks. The process of generating new blocks is referred to as *mining*, and nodes conducting mining activities are referred to as *miners*. To successfully mine, miners should find a solution called the *proof-of-work* (PoW) [2]. In Bitcoin, miners are required to solve a cryptographic puzzle finding a hash value to satisfy specific conditions such as a certain number of leading zeroes. To solve a puzzle, miners spend their computational power, and the miner who finds the solution obtains 12.5 coins and the transaction fees in the new block as a reward. In addition, Bitcoin has an average block interval of 10 minutes by adjusting the mining difficulty (i.e., the difficulty of the puzzles).

As Bitcoin has gained popularity, the transaction scalability issue has risen, and several solutions have been proposed to address the issue. However, there were also several conflicts over these solutions. As a result, in Aug. 2017, the Bitcoin system was split into the original Bitcoin (BTC) and Bitcoin Cash (BCH) [3], [4]. The key idea of BCH is to increase a maximum block size to process more transactions than BTC. However, even with different block size limits, they have compatible proof-of-work mechanisms with each other. Therefore, miners can freely alternate between BTC and BCH mining to boost their profits [5]. The mining profitability changes when the mining difficulty and coin price change, but some miners may be concerned only with the change in former because it is relatively easier to predict the former than the latter. More precisely, rational miners can decide which cryptocurrency is better to mine depending on the coin mining difficulty — BCH mining would be conducted by the miner only if the BCH mining difficulty is low compared to the BTC mining difficulty; otherwise, the miner does BTC mining rather than BCH mining. We call this miner's behavior "**fickle mining**" in this paper. Note that the fickle miner may change the coin to mine at a specific time period whenever the coin mining difficulty changes. Thus, fickle mining leads to instability of mining power, which may eventually cause unstable coin prices [5].

Game model and analysis. In this study, we aim to analyze the economics of fickle mining rigorously, which can later be extended to show how one coin can lead to a lack of loyal miners for other less valued coins. Here, a loyal miner represents one who conducts mining the less valued coin even after the coin mining difficulty increases. To study the economics of fickle mining, we propose a game theoretical framework of players who can conduct fickle mining between two coins (e.g., BTC and BCH). Moreover, our game model reflects *coin factions* that stick to mining their own coins, as they are interested in only the maintenance of their systems rather than the payoffs. Then we analyze Nash equilibria and dynamics in the game; two types of equilibria exist: the stable coexistence of two coins and the lack of loyal miners for the less valued coin. More specifically, in the latter case, only some factions (e.g., BITMAIN for BCH mining) remain as loyal miners for the less valued coin, and this fact can eventually make the coin system severely centralized, weakening its security. We describe the game model in Section IV and analyze the game in Section V.

Data analysis for BTC vs. BCH. Next, as a case study, we analyzed the mining power changes in BTC and BCH to see if our theoretical analysis matches with actual mining power changes. In this paper, we refer to the *Bitcoin system* as a coin system consisting of BTC and BCH. We examine the mining power history in the Bitcoin system from the release date of BCH until Dec. 2018 to 1) analyze which equilibrium its state has been moving to and 2) evaluate our theoretical analysis empirically. Our analysis results show that until the BCH mining difficulty adjustment algorithm changed (on Nov. 13, 2017), the Bitcoin state reached a lack of loyal miners for BCH. Therefore, BCH periodically became severely centralized before the update of the BCH protocol. For example, we observe a period when only five miners exist, of which two miners possess about 70 % power. However, since Nov. 13, 2017, the Bitcoin state has been close to coexistence because the change in the BCH mining difficulty adjustment algorithm with a shorter difficulty adjustment time interval (i.e., every block) has affected the game as an external factor.

Nevertheless, we explain that the state would still get closer to a lack of BCH loyal miners if *automatic mining*, in which miners automatically choose the most profitable coin to mine, is popularly used. Note that the main difference between fickle mining and automatic mining is that fickle miners *immediately* change their coin only when the mining difficulty changes while automatic miners can *immediately* change their coin when not only the mining difficulty but also the coin price changes. As a result, at the time of writing (Dec. 2018), if 5% of the total mining power of the Bitcoin system involves automatic mining, the current loyal miners for BCH would leave, weakening its security.

Data analysis for Bitcoin ABC vs. SV. As another case study in our game model, we also analyze the changes in the hash rate distributions of Bitcoin ABC and Bitcoin SV, before and after the recent "hash war" between those two coins. The analysis results of these case studies are presented in Section VI and VII.

Generalization. Moreover, we remark that our analysis can be generalized to any circumstance wherein two coins have compatible PoW mechanisms with each other. We believe that the generalized results bring new important angles in competitive coin markets; a coin can attempt to steal loyal miners from other rivalry coins that have compatible PoW mechanisms. In Section VIII, a risk of automatic mining and the way to intentionally reduce the number of loyal miners for other coins are described. Then, in Section IX, we discuss countermeasures and environmental factors that may make the actual coin states deviate from our game analysis.

In summary, our main contributions are as follows:

1) To analyze the economics of fickle mining, we first model a game between two coins, considering some coin factions that stick to mining their own coin.
2) We analyze Nash equilibria and dynamics in the game and find two types of equilibria: 1) stable coexistence of two coins and 2) a lack of loyal miners to the less valued coin. Then, we apply this game to the Bitcoin system.
3) To determine if real-world miners' behaviors follow our model, we investigate the mining power history in the Bitcoin system. Then we show that the state reached the lack of BCH loyal miners until Nov. 13, 2017, and we confirm that this fact periodically led the BCH system to be centralized and insecure. Moreover, for generalization, we also analyze the recent "hash war" situation between Bitcoin ABC and Bitcoin SV according to our game model.
4) We introduce a risk of automatic mining and predict that the current BCH loyal miners would leave when 5% of the total mining power in BTC and BCH involves automatic mining.
5) Finally, our game is generalized to any mining-compatible coins (e.g. Ethereum vs. Ethereum Classic). Therefore, our study brings a threat that one coin can intentionally steal loyal miners from other less valued coin.

II. Preliminary

A. Cryptocurrency

Many cryptocurrencies such as Bitcoin, Ethereum, and Litecoin adopt the PoW mechanism as a consensus algorithm. In the PoW mechanism, when a node solves a cryptographic puzzle, the node can generate and propagate a valid block. Then other nodes append the generated block to the existing blockchain. The puzzle is to find an inverse image of a hash function satisfying the certain condition, and thus the node should spend computational power to solve the cryptographic puzzle. The process of generating a block is called *mining*, and nodes participating in mining are called *miners*. In systems, the mining difficulty is adjusted to maintain the average time of generating one block. In particular, Bitcoin mining difficulty is adjusted to keep the average period of generating one block at 10 minutes. In addition, to incentivize mining, whenever a miner finds a valid block, the miner earns the reward for one block in compensation for the computational power spent. For example, currently, miners earn the block reward of 12.5 coins in the Bitcoin system when they find one block.

Many people have become involved in mining because of the incentive for mining, and specialized hardware for efficient mining such as application-specific integrated circuits (ASICs) has appeared. Based on the above reasons, the vast computational power is used for mining, and mining difficulty has increased significantly. Therefore, it should take a *solo miner*, who mines alone, a significantly long time to find a valid block, and this causes solo miners to wait for a long time to earn block rewards. To reduce not only node costs and but also the variance of their rewards, *mining pools* where miners gather together for mining have been organized. Most pools are composed of workers and a manager. The manager gives puzzles to workers, and they solve the puzzles. If a worker solves a given puzzle, the block reward is distributed to the workers in the pool.

In the past years, there have been many attacks on and problems with cryptocurrency systems, and these attacks or problems have even caused cryptocurrency systems to split. For example, because Bitcoin has become a popular cryptocurrency, the system needs to provide high transaction throughput. To address the scalability issue, several solutions such as Segregated Witness [6] and unlimited block size have been proposed. Because of the debate on the proposed solutions, Bitcoin was eventually split into BTC and BCH in early Aug. 2017. Even though BCH chose to increase the block size limit in order to allow more transactions per block, the mining protocol of BCH was designed to be compatible with that of BTC. Therefore, miners can conduct both BTC and BCH mining with one hardware device.

B. Fickle mining

Before Nov. 13, 2017, BCH adjusted the mining difficulty every 2016 block to ensure that the average time period for generating a block is 10 minutes, like in the case of BTC. In doing so, if the time required for generating past 2016 blocks is longer than two weeks, the mining difficulty decreases, and miners can generate subsequent blocks more easily. In addition, BCH added a new difficulty adjustment algorithm called emergency difficulty adjustment (EDA) [7] to decrease the mining difficulty without waiting for 2016 blocks to be generated when it is significantly difficult to find a valid block.

Because BTC and BCH have a PoW mechanism compatible with each other, miners can freely switch between them depending on the mining difficulty and the coin price. However, because the change in coin price is hard to predict, some miners immediately change their coin only when mining difficulty changes, where we call this behavior *fickle mining*. Concretely, the fickle miners first conduct BTC mining, observing the changes in the mining difficulties of BTC and BCH. Then, if the BCH mining difficulty is low, they immediately shift to BCH mining. When the BCH mining difficulty increases again thanks to its difficulty adjustment algorithm, fickle miners immediately shift to BTC mining. Fickle mining can boost profits of miners; however, this behavior might cause instability of both BTC and BCH.

This mining behavior was easily observed in Bitcoin when we monitored the mining power in pools. We collected mining power history data over the course of a week from two popular pools: ViaBTC [8] and BTC.com [9]. These two pools support both BTC and BCH mining; miners in the pools can choose either BTC or BCH mining by just clicking one button. Figure 1 represents the mining power data of ViaBTC and BTC.com for a week. In the figure, the grey regions show movements of mining power from BTC to BCH mining.

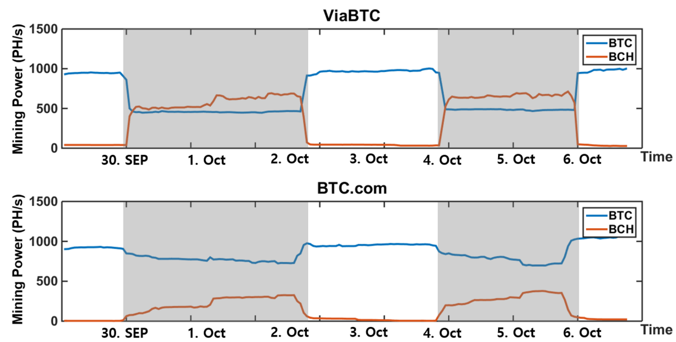

Figure 1. Mining power history of ViaBTC and BTC.com (Sep. 29, 2017 ∼ Oct. 6, 2017). The grey regions represent movements of mining power from BTC to BCH.

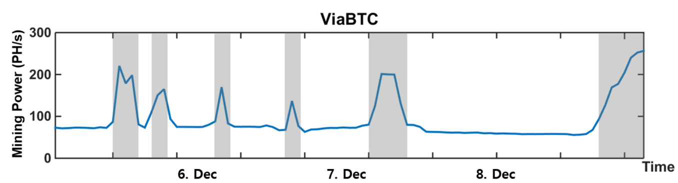

Figure 2. Mining power history of ViaBTC (Dec. 5, 2017 ∼ Dec. 8, 2017). Grey regions represent movements of mining power from BTC to BCH. Note that we only displayed the mining power history of ViaBTC because BTC.com did not evidently execute fickle mining for this period.

As fickle mining causes a sudden increase in mining power as shown in the grey zones of Figure 1, many blocks were generated quite quickly in the BCH system. For example, in the BCH system, 2016 blocks were generated within only three days in each grey zone. This caused the blockchain of BCH to be thousands of blocks ahead of BTC, and the halving time of the block reward in BCH was brought forward. To address this issue, BCH performed another hard fork on Nov. 13, 2017 [10]. Currently, BCH adjusts the difficulty for *each* block based on the previous 144 blocks as a moving window [11]. To determine if it is possible that miners conduct fickle mining even after the hard fork of Nov. 13, 2017, we investigated the BCH mining power data of ViaBTC for four days (Dec. 5, 2017 ∼ Dec. 8, 2017). Figure 2 represents the BCH mining power data of ViaBTC during this time period; as is evident from the figure, some miners still conduct fickle mining. Because the BCH mining difficulty is more quickly adjusted than before the hard fork of BCH, fickle miners should switch their mining power more quickly than before the hard fork. Indeed, fickle mining can occur in any mining difficulty adjustment algorithm.

III. Related work

In this section, we review previous studies related to mining in PoW systems. Kroll et al. considered the Bitcoin mining process as a game among multiple players [12] and showed that a miner possessing 51% mining power can be motivated to disrupt the Bitcoin system. Several works [13], [14] modeled and analyzed a game between two pools that can launch denial of service attacks against each other. Eyal and Sirer introduced the selfish mining strategy, where a malicious miner successfully mines blocks but does not immediately broadcast the blocks; instead, the attacker temporarily withholds the block [15]. Many researchers have intensively studied ways to optimize and extend selfish mining [16], [17], [18], [19]. Bonneau introduced bribery attacks as a way for an attacker to increase her mining power [20]. Lewenberg et al. considered a mechanism of sharing rewards among pool miners as a cooperative game [21]. In 2015, Eyal modeled a game between two pools that execute block withholding (BWH) attacks [22]. As a concurrent work, Luu et al. [23] modeled a power splitting game to find an optimized strategy for a BWH attacker. Kwon et al. [24] proposed a new attack called a fork after withholding (FAW) attack against pools [24]. Also, several works [25], [26] analyzed a transaction-fee regime in PoW systems, where miners receive incentives for mining as transaction fees. Moreover, because many cryptocurrencies are competing with each other, there can be another incentive to execute 51% attacks. Considering this fact, Bonneau revisited the 51% attack with some basic analysis [27].

Recently, Ma et al. [28] considered a mining game of multiple miners and concluded that openness of the Bitcoin system causes the need for vast mining power. Another study [29] examined the relation between the Bitcoin/USD exchange rate and Bitcoin mining power. They first proposed an industry equilibrium model to forecast the mining power depending on the Bitcoin/USD exchange rate. Then, they showed that the real mining power data and simulated mining power according to their model are similar. Our study focuses on the relation between two coins that have compatible PoW mechanisms with each other and the miners' behavior between two coins. Furthermore, our model can be used to forecast the ratio of mining power between two coins. To the best of our knowledge, this is the first to study the effects of fickle mining.

IV. Model

In this section, we formally model a game to represent fickle mining between two coins.

A. Notation and assumptions

We consider two coins, $coin_{\mathtt{A}}$ and $coin_{\mathtt{B}}$, which have compatible PoW mechanisms with each other. In this case, a miner with a hardware device can alternately conduct mining of $coin_{\mathtt{A}}$ and $coin_{\mathtt{B}}$; that is, he can conduct fickle mining between them. Meanwhile, a $coin_{\mathtt{B}}$-faction can stick to $coin_{\mathtt{B}}$-mining rather than fickle mining or $coin_{\mathtt{A}}$-mining to maintain its own coin, and the set of $coin_{\mathtt{B}}$-factions sticking to $coin_{\mathtt{B}}$-mining is denoted by $\Omega_{\mathtt{stick}}$. For example, in the case where BCH is $coin_{\mathtt{B}}$, BITMAIN [30], one of the main supporters of BCH, may belong to $\Omega_{\mathtt{stick}}$. We aim to formalize a game considering the fickle mining and $\Omega_{\mathtt{stick}}$.

The proposed game consists of many players (i.e., miners), where the set of all players is denoted by Ω. Player $i \in \Omega$ chooses one of three strategies, $s_i \in \{\mathcal{F}, \mathcal{A}, \mathcal{B}\}$: Fickle mining ($\mathcal{F}$), $coin_{\mathtt{A}}$-only mining ($\mathcal{A}$), and $coin_{\mathtt{B}}$-only mining ($\mathcal{B}$). The payoff function of player i is denoted by $U_i : \{\mathcal{F}, \mathcal{A}, \mathcal{B}\}^n \to \mathbb{R}$, which we will formally define later as well as fickle mining. We also define three sets $\mathcal{M}_{\mathcal{F}} = \{i \in \Omega \,|\, s_i = \mathcal{F}\}$, $\mathcal{M}_{\mathcal{A}} = \{i \in \Omega \,|\, s_i = \mathcal{A}\}$, and $\mathcal{M}_{\mathcal{B}} = \{i \in \Omega \,|\, s_i = \mathcal{B}\}$, indicating a set of players who conduct fickle mining, $coin_{\mathtt{A}}$-only mining, and $coin_{\mathtt{B}}$-only mining, respectively. Note that $\Omega_{\mathtt{stick}}$ is a subset of $\mathcal{M}_{\mathcal{B}}$ because players in $\Omega_{\mathtt{stick}}$ always choose strategy $\mathcal{B}$. The sum of mining powers in $coin_{\mathtt{A}}$ and $coin_{\mathtt{B}}$ is regarded as 1; mining power of a coin is expressed as a ratio to the total mining power. The mining power possessed by player i is denoted by c_i, and the total computational power possessed by $\Omega_{\mathtt{stick}}$ is denoted by $c_{\mathtt{stick}}$. We also define $c_{\mathtt{max}}$ as the maximum of $\{c_i \,|\, i \in \Omega \backslash \Omega_{\mathtt{stick}}\}$. Moreover, because our game analysis result would depend on the computational power possessed by players, we use the notation $\mathcal{G}(\boldsymbol{c}, c_{\mathtt{stick}})$ to refer to the game, where $\boldsymbol{c}$ indicates a vector of computational power possessed by players except for $\Omega_{\mathtt{stick}}$ (i.e., $\boldsymbol{c} = (c_i)_{i \in \Omega \backslash \Omega_{\mathtt{stick}}}$). Lastly, we denote the total mining power of $\mathcal{M}_{\mathcal{F}}$, $\mathcal{M}_{\mathcal{A}}$, and $\mathcal{M}_{\mathcal{B}}$ as $r_{\mathcal{F}}$ (i.e., $\sum_{i \in \mathcal{M}_{\mathcal{F}}} c_i$), $r_{\mathcal{A}}$ (i.e., $\sum_{i \in \mathcal{M}_{\mathcal{A}}} c_i$), and $r_{\mathcal{B}}$ (i.e., $\sum_{i \in \mathcal{M}_{\mathcal{B}}} c_i$), respectively. Observe that $r_{\mathcal{A}} = 1 - r_{\mathcal{F}} - r_{\mathcal{B}}$ and $c_{\mathtt{stick}} \leq r_{\mathcal{B}}$. Namely, $(r_{\mathcal{F}}, r_{\mathcal{B}})$ represents the full status of mining powers where $r_{\mathcal{B}}$ is not less than $c_{\mathtt{stick}}$.

For the analysis of the game, we assume the following:

Assumption 1. *A miner conducts either only $coin_{\mathtt{A}}$ or $coin_{\mathtt{B}}$-mining (not both) at each time instance; for example, an ASIC miner cannot execute both BTC and BCH mining simultaneously. However, their choices can be time-varying; that is, miners can change their coin to mine.*

Assumption 2. *The price of 1 $coin_{\mathtt{B}}$ is equal to that of k $coin_{\mathtt{A}}$. We assume that $0 < k \leq 1$ without loss of generality. In addition, rewards for mining a block in both coins are 1 $coin_{\mathtt{A}}$ and 1 $coin_{\mathtt{B}}$, respectively.*

Assumption 3. *In both $coin_{\mathtt{A}}$ and $coin_{\mathtt{B}}$ systems, mining difficulties are adjusted to maintain the average period of generating a block as the same specific time period, which we denote by 1 P_{ag} time and regard as a time unit; for example, 1 P_{ag} = 10 minutes in the Bitcoin system. Furthermore, we consider a generalized model in which mining difficulties of $coin_{\mathtt{A}}$ and $coin_{\mathtt{B}}$ are adjusted in proportion to the mining power for the previous time window, and we consider a normalized difficulty. Thus, if x mining power has been engaged in coin mining, the mining difficulty would be x. More precisely, in*

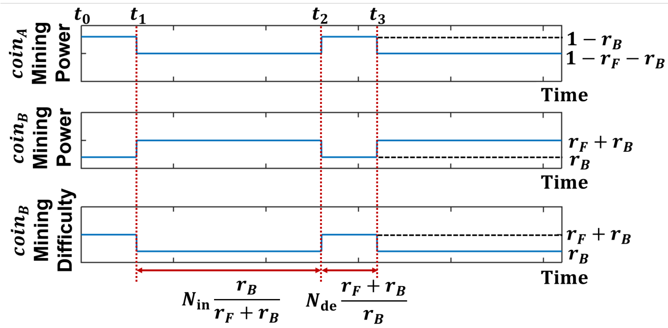

Figure 3. Changes in the mining power of $coin_{\mathtt{A}}$ and $coin_{\mathtt{B}}$, and mining difficulty of $coin_{\mathtt{B}}$.

our model, the coin mining difficulty decreases and increases again, considering the generation time of a specific number of blocks since the last update of coin mining difficulty. In particular, for the mining difficulty of $coin_{\mathtt{B}}$, we denote the number of considered blocks when the $coin_{\mathtt{B}}$-mining difficulty decreases and increases as $N_{\mathtt{de}}$ and $N_{\mathtt{in}}$, respectively.[1] *Note that $N_{\mathtt{de}}$ and $N_{\mathtt{in}}$ cannot be zero. In the case of BTC and Litecoin, $N_{\mathtt{de}}$ and $N_{\mathtt{in}}$ are 2016.*

As described previously, a fickle miner may change the preferred coin when the coin mining difficulty changes. Here we define fickle mining formally.

Definition IV.1 (Fickle mining)**.** *Let $D_{\mathtt{A}}$ and $D_{\mathtt{B}}$ denote the $coin_{\mathtt{A}}$ and $coin_{\mathtt{B}}$-mining difficulties, respectively. If $D_{\mathtt{B}} < \min\{r_{\mathcal{F}} + r_{\mathcal{B}}, k \cdot D_{\mathtt{A}}\}$ or $D_{\mathtt{B}} \leq r_{\mathcal{B}}$ when $D_{\mathtt{A}}$ or $D_{\mathtt{B}}$ is updated, fickle miners ($\mathcal{M}_{\mathcal{F}}$) decide to conduct $coin_{\mathtt{B}}$-mining until $D_{\mathtt{A}}$ or $D_{\mathtt{B}}$ is adjusted again. Otherwise, they conduct $coin_{\mathtt{A}}$-mining.*

We also emphasize that if $r_{\mathcal{F}}$ is 0, no miner engages in fickle mining, and mining powers of $coin_{\mathtt{A}}$ and $coin_{\mathtt{B}}$ are stably maintained. On the other hand, if $r_{\mathcal{B}}$ is $c_{\mathtt{stick}}$, only $coin_{\mathtt{B}}$-factions $\Omega_{\mathtt{stick}}$ would conduct $coin_{\mathtt{B}}$-mining after an increase in the mining difficulty of $coin_{\mathtt{B}}$. In other words, in this case, only the factions remain as *loyal miners* for $coin_{\mathtt{B}}$. Therefore, if the number of such factions ($|\Omega_{\mathtt{stick}}|$) is small, the state would be a lack of loyal miners. Note that loyal miners refer to players who continue to conduct $coin_{\mathtt{B}}$-mining even after an increase in $coin_{\mathtt{B}}$-mining. In particular, if all $coin_{\mathtt{B}}$-factions stop $coin_{\mathtt{B}}$-mining for higher payoff (i.e., $|\Omega_{\mathtt{stick}}| = 0$), $r_{\mathcal{B}}$ is 0, and no player conducts $coin_{\mathtt{B}}$-mining after an increase in the mining difficulty of $coin_{\mathtt{B}}$. Note that the $coin_{\mathtt{B}}$-mining difficulty cannot decrease in this case because $N_{\mathtt{de}}$ cannot be zero. Therefore, the case $r_{\mathcal{B}} = 0$ indicates the complete downfall of $coin_{\mathtt{B}}$ while only $coin_{\mathtt{A}}$ survives.

Parameters used in this paper are summarized in Table I. The last parameter in the table will be introduced later.

Table I
LIST OF PARAMETERS.

$\Omega_{\mathtt{stick}}$	The set of $coin_{\mathtt{B}}$-factions sticking to $coin_B$ mining to maintain their own coin
Ω	The set of all players
s_i	Player i's strategy
U_i	Player i's payoff
$\mathcal{F}$, $\mathcal{A}$, $\mathcal{B}$	Fickle, $coin_{\mathtt{A}}$-only, $coin_{\mathtt{B}}$-only mining
$\mathcal{M}_{\mathcal{F}}$, $\mathcal{M}_{\mathcal{A}}$, $\mathcal{M}_{\mathcal{B}}$	The set of players with $\mathcal{F}$, $\mathcal{A}$, $\mathcal{B}$
c_i	Computational power of player i
$c_{\mathtt{stick}}$	Computational power possessed by $\Omega_{\mathtt{stick}}$
$c_{\max}$	The maximum of $\{c_i \mid i \in \Omega \backslash \Omega_{\mathtt{stick}}\}$
$\boldsymbol{c}$	The vector of computational power possessed by players in $\Omega \backslash \Omega_{\mathtt{stick}}$
$\mathcal{G}(\boldsymbol{c}, c_{\mathtt{stick}})$	The game of players and $\Omega_{\mathtt{stick}}$ with computational power $\boldsymbol{c}$ and $c_{\mathtt{stick}}$
$r_{\mathcal{F}}, r_{\mathcal{A}}, r_{\mathcal{B}}$	The total computational power fraction of $\mathcal{M}_{\mathcal{F}}$, $\mathcal{M}_{\mathcal{A}}$, $\mathcal{M}_{\mathcal{B}}$
k	The relative price of $coin_{\mathtt{B}}$ to $coin_{\mathtt{A}}$
$P_{\mathtt{ag}}$	The time unit representing the average period of generating one block
$N_{\mathtt{de}}, N_{\mathtt{in}}$	The number of considered past blocks when the mining difficulty of $coin_{\mathtt{B}}$ decreases or increases
$D_{\mathtt{A}}, D_{\mathtt{B}}$	The mining difficulty of $coin_{\mathtt{A}}$, $coin_{\mathtt{B}}$
$\mathcal{E}(\boldsymbol{c}, c_{\mathtt{stick}})$	The set of all Nash equilibrium in $\mathcal{G}(\boldsymbol{c}, c_{\mathtt{stick}})$

Illustration of fickle mining. Figure 3 illustrates a stream of mining power in $coin_{\mathtt{A}}$ and $coin_{\mathtt{B}}$, as well as the mining difficulty of $coin_{\mathtt{B}}$ over time, caused by the strategies of players.
- Time t_0 : At the beginning, $1 - r_{\mathcal{B}}$ and $r_{\mathcal{B}}$ mining powers are used for $coin_{\mathtt{A}}$ and $coin_{\mathtt{B}}$-mining, respectively.
- Time t_1 : The mining difficulty of $coin_{\mathtt{B}}$ decreases because it is relatively difficult to find PoWs with $r_{\mathcal{B}}$ mining power. At the moment, $\mathcal{M}_{\mathcal{F}}$ shifts from $coin_{\mathtt{A}}$ to $coin_{\mathtt{B}}$, and each of $1 - r_{\mathcal{F}} - r_{\mathcal{B}}$ and $r_{\mathcal{F}} + r_{\mathcal{B}}$ mining powers is used for $coin_{\mathtt{A}}$ and $coin_{\mathtt{B}}$-mining, respectively.
- Time t_2 : Because the mining difficulty of $coin_{\mathtt{B}}$ is again adjusted (increases) after $N_{\mathtt{in}}$ blocks are found in the $coin_{\mathtt{B}}$ system since the last adjustment of the mining difficulty of $coin_{\mathtt{B}}$, the mining difficulty of $coin_{\mathtt{B}}$ would increase after $\frac{N_{\mathtt{in}} r_{\mathcal{B}}}{r_{\mathcal{F}} + r_{\mathcal{B}}}$ $P_{\mathtt{ag}}$ time since it takes $\frac{r_{\mathcal{B}}}{r_{\mathcal{F}} + r_{\mathcal{B}}}$ $P_{\mathtt{ag}}$ to find one valid block on average. Then, $\mathcal{M}_{\mathcal{F}}$ shifts again from $coin_{\mathtt{B}}$ to $coin_{\mathtt{A}}$ and conducts $coin_{\mathtt{A}}$-mining until the mining difficulty of $coin_{\mathtt{B}}$ decreases.
- Time t_3 : Until when the mining difficulty of $coin_{\mathtt{B}}$ decreases after $N_{\mathtt{de}}$ blocks are found in the $coin_{\mathtt{B}}$ system, $\mathcal{M}_{\mathcal{F}}$ would conduct $coin_{\mathtt{A}}$-mining (for $\frac{N_{\mathtt{de}}(r_{\mathcal{F}} + r_{\mathcal{B}})}{r_{\mathcal{B}}}$ $P_{\mathtt{ag}}$ time).
- This process is continually repeated.

B. Payoff function

Next, we describe payoff functions for our game model. All payoffs are expressed as a unit of $coin_{\mathtt{A}}$ and are calculated as a profit density, which is defined as an average earned reward for 1 $P_{\mathtt{ag}}$ time divided by the player's mining power. In other words, if player i earns a reward R for 1 $P_{\mathtt{ag}}$ time on average, the payoff would be $\frac{R}{c_i}$. Player i's payoff function $U_i(s_i, \mathbf{s_{-i}})$

[1] In Section VI, we will show that our results can be applied to the coin system regardless of the mining difficulty adjustment algorithm of $coin_{\mathtt{B}}$.

is expressed as follows:

$$U_i(s_i, \mathbf{s_{-i}}) = \begin{cases} U_{\mathcal{F}}(r_{\mathcal{F}}, r_{\mathcal{B}}) \text{ if } s_i = \mathcal{F} \\ U_{\mathcal{A}}(r_{\mathcal{F}}, r_{\mathcal{B}}) \text{ if } s_i = \mathcal{A} \\ U_{\mathcal{B}}(r_{\mathcal{F}}, r_{\mathcal{B}}) \text{ if } s_i = \mathcal{B} \end{cases} \quad (1)$$

where $\mathbf{s_{-i}}$ indicates other players' strategies. Here, it suffices to define $U_{\mathcal{F}}, U_{\mathcal{A}}, U_{\mathcal{B}}$ in the range $0 < r_{\mathcal{F}} \leq 1$, $0 < r_{\mathcal{A}} \leq 1$, and $0 < r_{\mathcal{B}} \leq 1$, respectively; for example, $U_{\mathcal{F}}$ would be defined when $s_i = \mathcal{F}$ (i.e, a fickle miner exists, and $0 < r_{\mathcal{F}}$).

First, we define the payoff $U_{\mathcal{F}}$ for a player in $\mathcal{M}_{\mathcal{F}}$. As shown in Figure 3, $\mathcal{M}_{\mathcal{F}}$ conducts $coin_{\mathtt{B}}$-mining for $\frac{N_{\mathtt{in}} r_{\mathcal{B}}}{r_{\mathcal{F}}+r_{\mathcal{B}}}$ $P_{\mathtt{ag}}$ time. Therefore, a player in $\mathcal{M}_{\mathcal{F}}$ earns the profit $\frac{k \cdot c_i}{r_{\mathcal{B}}}$ per 1 $P_{\mathtt{ag}}$ time on average for $\frac{N_{\mathtt{in}} r_{\mathcal{B}}}{r_{\mathcal{F}}+r_{\mathcal{B}}}$ $P_{\mathtt{ag}}$ time. After that, $\mathcal{M}_{\mathcal{F}}$ conducts $coin_{\mathtt{A}}$-mining for $\frac{N_{\mathtt{de}}(r_{\mathcal{F}}+r_{\mathcal{B}})}{r_{\mathcal{B}}}$ $P_{\mathtt{ag}}$ time during which a player in $\mathcal{M}_{\mathcal{F}}$ earns the following profit per 1 $P_{\mathtt{ag}}$ time on average:

$$\mathrm{AP}_{\mathcal{F}} := c_i \frac{\frac{N_{\mathtt{in}} r_{\mathcal{B}}}{r_{\mathcal{F}}+r_{\mathcal{B}}} + \frac{N_{\mathtt{de}}(r_{\mathcal{F}}+r_{\mathcal{B}})}{r_{\mathcal{B}}}}{(1-r_{\mathcal{F}}-r_{\mathcal{B}})\frac{N_{\mathtt{in}} r_{\mathcal{B}}}{r_{\mathcal{F}}+r_{\mathcal{B}}} + (1-r_{\mathcal{B}})\frac{N_{\mathtt{de}}(r_{\mathcal{F}}+r_{\mathcal{B}})}{r_{\mathcal{B}}}}. \quad (2)$$

The above formulation is due to the fact that mining powers $1-r_{\mathcal{F}}-r_{\mathcal{B}}$ and $1-r_{\mathcal{B}}$ engage in $coin_{\mathtt{A}}$-mining for $\frac{N_{\mathtt{in}} r_{\mathcal{B}}}{r_{\mathcal{F}}+r_{\mathcal{B}}}$ $P_{\mathtt{ag}}$ and $\frac{N_{\mathtt{de}}(r_{\mathcal{F}}+r_{\mathcal{B}})}{r_{\mathcal{B}}}$ $P_{\mathtt{ag}}$ times, respectively, and thus, the second factor in the right-hand side of (2) represents an inverse number of the mining difficulty of $coin_{\mathtt{A}}$. Consequently, the payoff of a player in $\mathcal{M}_{\mathcal{F}}$ can be expressed as

$$U_{\mathcal{F}}(r_{\mathcal{F}}, r_{\mathcal{B}}) = \left(\frac{k \cdot c_i}{r_{\mathcal{B}}} \cdot \frac{N_{\mathtt{in}} r_{\mathcal{B}}}{r_{\mathcal{F}}+r_{\mathcal{B}}} + \mathrm{AP}_{\mathcal{F}} \times \frac{N_{\mathtt{de}}(r_{\mathcal{F}}+r_{\mathcal{B}})}{r_{\mathcal{B}}}\right) \times Z,$$

where

$$Z = \frac{1}{c_i \left(\frac{N_{\mathtt{in}} r_{\mathcal{B}}}{r_{\mathcal{F}}+r_{\mathcal{B}}} + \frac{N_{\mathtt{de}}(r_{\mathcal{F}}+r_{\mathcal{B}})}{r_{\mathcal{B}}}\right)}.$$

Next, we provide payoffs $U_{\mathcal{A}}$ and $U_{\mathcal{B}}$ as follows:

$$U_{\mathcal{A}}(r_{\mathcal{F}}, r_{\mathcal{B}}) = \frac{\mathrm{AP}_{\mathcal{F}}}{c_i},$$

$$U_{\mathcal{B}}(r_{\mathcal{F}}, r_{\mathcal{B}}) = \left(\frac{kN_{\mathtt{in}}}{r_{\mathcal{F}}+r_{\mathcal{B}}} + \frac{kN_{\mathtt{de}}}{r_{\mathcal{B}}}\right) \times c_i \cdot Z,$$

where we observe that a player in $\mathcal{M}_{\mathcal{B}}$ earns the profit $\frac{k \cdot c_i}{r_{\mathcal{B}}}$ per 1 $P_{\mathtt{ag}}$ for $\frac{N_{\mathtt{in}} r_{\mathcal{B}}}{r_{\mathcal{F}}+r_{\mathcal{B}}}$ $P_{\mathtt{ag}}$ time and profit $\frac{k \cdot c_i}{r_{\mathcal{F}}+r_{\mathcal{B}}}$ per 1 $P_{\mathtt{ag}}$ for $\frac{N_{\mathtt{de}}(r_{\mathcal{F}}+r_{\mathcal{B}})}{r_{\mathcal{B}}}$ $P_{\mathtt{ag}}$ time, on average.

V. Game analysis

In this section, we analyze Nash equilibria and dynamics in game $\mathcal{G}(\boldsymbol{c}, c_{\mathtt{stick}})$.

A. Equilibrium in game $\mathcal{G}(\boldsymbol{c}, c_{\mathtt{stick}})$

Characterization of equilibria. Before finding Nash equilibria of $\mathcal{G}(\boldsymbol{c}, c_{\mathtt{stick}})$, we define a pure Nash equilibrium.

Definition V.1 (Pure Nash equilibrium)**.** *A strategy vector* $\mathbf{s} = (s_1, s_2, \cdots s_n)$ *is a Nash equilibrium if*

$$U_i(\mathbf{s}) = \max_{s'_i \in \{\mathcal{F}, \mathcal{A}, \mathcal{B}\}} U_i(s'_i, \mathbf{s_{-i}}), \qquad \textit{for all } i.$$

At an equilibrium, all rational players would not change their strategy, that is, $r_{\mathcal{F}}$ and $r_{\mathcal{B}}$ are not updated. We map a strategy vector $\mathbf{s} = (s_1, s_2, \cdots s_n)$ to state $(r_{\mathcal{F}}, r_{\mathcal{B}})$ and denote by $\mathcal{E}(\boldsymbol{c}, c_{\mathtt{stick}})$ the set of all Nash equilibria in $\mathcal{G}(\boldsymbol{c}, c_{\mathtt{stick}})$. We first determine the dynamics of player i with small c_i through Lemma V.1 to establish the characterization of $\mathcal{E}(\boldsymbol{c}, c_{\mathtt{stick}})$.

Lemma V.1. *There is $\varepsilon > 0$ such that, any player i possessing $c_i < \varepsilon$ does not change its strategy at state $(r_{\mathcal{F}}, r_{\mathcal{B}})$ if and only if*

$$(r_{\mathcal{F}}, r_{\mathcal{B}}) = \begin{cases} (f_\varepsilon(c_{\mathtt{stick}}), c_{\mathtt{stick}}) & \textit{if} c_{\mathtt{stick}} > 0, \\ \left(\frac{k}{2} + \frac{\sqrt{N_{\mathtt{de}}{}^2 k^2 + 4N_{\mathtt{de}} N_{\mathtt{in}}(k \cdot c_i - c_i^2)}}{2N_{\mathtt{de}}} \leq r_{\mathcal{F}} \leq 1, 0\right) & \textit{otherwise,} \end{cases}$$

where f_ε is a decreasing function of which input is $c_{\mathtt{stick}}$ and output ranges between 0 and $1 - c_{\mathtt{stick}}$. Parameters $k, N_{\mathtt{de}}$, and $N_{\mathtt{in}}$ are defined in Assumption 2 and 3.

Note that $f_\varepsilon(c_{\mathtt{stick}})$ is $1 - c_{\mathtt{stick}}$ for a small value of $c_{\mathtt{stick}}$ while $f_\varepsilon(c_{\mathtt{stick}})$ is 0 for a large value of $c_{\mathtt{stick}}$. The above lemma implies that, considering miners with small computational power, if a Nash equilibrium exists, only $\Omega_{\mathtt{stick}}$ would remain as loyal miners to $coin_{\mathtt{B}}$ in the equilibrium. This is because $(r_{\mathcal{F}}, r_{\mathcal{B}})$ would continually change when $r_{\mathcal{B}}$ is greater than $c_{\mathtt{stick}}$. From Lemma V.1, we can characterize the set $\mathcal{E}(\boldsymbol{c}, c_{\mathtt{stick}})$ as stated in Theorem V.2. We present the proof of Lemma V.1 and Theorem V.2 in the full version of this paper [31].

Theorem V.2. *There is $\varepsilon > 0$ such that, when $c_{\mathtt{max}} < \varepsilon$, the set $\mathcal{E}(\boldsymbol{c}, c_{\mathtt{stick}})$ is as follows.*

$$\mathcal{E}(\boldsymbol{c}, c_{\mathtt{stick}}) = \begin{cases} \{(r_{\mathcal{F}}, r_{\mathcal{B}}) : X \leq r_{\mathcal{F}} \leq 1, r_{\mathcal{B}} = 0\} & \textit{if} c_{\mathtt{stick}} = 0, \\ \{(1 - c_{\mathtt{stick}}, c_{\mathtt{stick}})\} & \textit{else if} c_{\mathtt{stick}} < x, \\ \{(0, c_{\mathtt{stick}})\} & \textit{else if} c_{\mathtt{stick}} > y, \end{cases}$$

where

$$X = \max_{i \in \Omega \setminus \Omega_{\mathtt{stick}}} \left\{ \frac{k}{2} + \frac{\sqrt{N_{\mathtt{de}}{}^2 k^2 + 4N_{\mathtt{de}} N_{\mathtt{in}}(k \cdot c_i - c_i^2)}}{2N_{\mathtt{de}}} \right\},$$

x and y $(> x)$ range between 0 and 1.

As described above, Theorem V.2 shows that, in a game where players except for $\Omega_{\mathtt{stick}}$ possess small computational power, there exist only Nash equilibria where the $coin_{\mathtt{B}}$-factions sticking to $coin_{\mathtt{B}}$-mining are loyal miners for $coin_{\mathtt{B}}$. In the case where $c_{\mathtt{stick}}$ is small, we can certainly see that the overall health of the $coin_{\mathtt{B}}$ system would be weakened in terms of scalability, decentralization, and security, which will be discussed in more detail in Section VII-A. Indeed, even if $c_{\mathtt{stick}}$ is large, the case where $r_{\mathcal{B}}$ is equal to $c_{\mathtt{stick}}$ would make the $coin_{\mathtt{B}}$ system significantly centralized because only a few players possessing large power are loyal miners to $coin_{\mathtt{B}}$ (this example is presented in Section VII-B). In particular, if $\Omega_{\mathtt{stick}}$ is empty, no miner exists in the $coin_{\mathtt{B}}$ system in all Nash equilibria. Remark that this case indicates the complete downfall of $coin_B$. As a result, Theorem V.2 implies that fickle mining can be dangerous.

When players possess infinitesimal mining power. Under the game $\mathcal{G}(\boldsymbol{c}, c_{\mathtt{stick}})$, it is not easy to analyze movement of state $(r_{\mathcal{F}}, r_{\mathcal{B}})$ (this movement will be used for data analysis in

Section VII) due to a large degree of freedom in $\boldsymbol{c}$. Thus, we further assume that players except for $\Omega_{\texttt{stick}}$ (i.e., $\Omega\backslash\Omega_{\texttt{stick}}$) possess infinitesimal computational power (i.e., $\|\boldsymbol{c}\|_2 \approx 0$). We show that this assumption is reasonable by analyzing the real-world dataset in the Bitcoin system (see Section VI). We again study the equilibria of $\mathcal{G}(\boldsymbol{c}, c_{\texttt{stick}})$ in this case.

Theorem V.3. *When players except for $\Omega_{\texttt{stick}}$ possess infinitesimal mining power, the set $\mathcal{E}(\boldsymbol{c}, c_{\texttt{stick}})$ is as follows.*

$$\mathcal{E}(\boldsymbol{c}, c_{\texttt{stick}}) =
\begin{cases}
\left\{\left(0, \frac{k}{k+1}\right)\right\} \cup \{(r_{\mathcal{F}}, r_{\mathcal{B}}) : k \le r_{\mathcal{F}} \le 1, r_{\mathcal{B}} = 0\} \\
\qquad \textit{if } c_{\texttt{stick}} = 0 \textit{ (Case 1)}, \\
\left\{\left(0, \frac{k}{k+1}\right)\right\} \cup \{(1 - c_{\texttt{stick}}, c_{\texttt{stick}})\} \\
\qquad \textit{else if } c_{\texttt{stick}} \le \alpha \textit{ (Case 2)}, \\
\left\{\left(0, \frac{k}{k+1}\right)\right\} \cup \{(\beta, c_{\texttt{stick}})\} \\
\qquad \textit{else if } \alpha < c_{\texttt{stick}} \le \frac{k}{k+1} \textit{ (Case 3)}, \\
\{(0, c_{\texttt{stick}})\} \quad \textit{otherwise (Case 4)}
\end{cases} \tag{3}$$

Here, α and β are defined in Section V-B.

We present the proof of Theorem V.3 in the full version of this paper [31]. Comparing with Theorem V.2, the state $(0, \frac{k}{k+1})$ also becomes another Nash equilibrium when the computational power possessed by players (except for $\Omega_{\texttt{stick}}$) is infinitesimal. Note that this state indicates the stable coexistence of $coin_{\texttt{A}}$ and $coin_{\texttt{B}}$. Indeed, when $\|\boldsymbol{c}\|_2$ is closer to 0, the difference among payoffs of players in $\mathcal{M}_{\mathcal{F}}$, $\mathcal{M}_{\mathcal{A}}$, and $\mathcal{M}_{\mathcal{B}}$ would also be closer to 0 at the state $(0, \frac{k}{k+1})$. Therefore, under the assumption that players possess infinitesimal power, payoffs of players in $\mathcal{M}_{\mathcal{F}}$, $\mathcal{M}_{\mathcal{A}}$, and $\mathcal{M}_{\mathcal{B}}$ are the same at the state $(0, \frac{k}{k+1})$ while the mining difficulties of $coin_{\texttt{A}}$ and $coin_{\texttt{B}}$ are maintained as $\frac{1}{k+1}$ and $\frac{k}{k+1}$, respectively. Meanwhile, at the remaining equilibria except for the state $(0, \frac{k}{k+1})$, only the $coin_{\texttt{B}}$-factions $\Omega_{\texttt{stick}}$ conduct $coin_{\texttt{B}}$-mining after the $coin_{\texttt{B}}$-mining difficulty increases. In particular, if no $coin_{\texttt{B}}$-faction sticking to $coin_{\texttt{B}}$-mining exists, loyal mining power to $coin_{\texttt{B}}$ is 0 in the Nash equilibria. Note that, in this case, $\mathcal{M}_{\mathcal{F}}$ and $\mathcal{M}_{\mathcal{A}}$ would continuously conduct $coin_{\texttt{A}}$-mining, because the mining difficulty of $coin_{\texttt{B}}$ has not decreased after the previous increase in difficulty. These players would not also change their strategy because the mining difficulty of $coin_{\texttt{B}}$ increases to a significantly high value due to the heavy occurrence of fickle mining.

Example. Considering the case $c_{\texttt{stick}} = 0$, we give an example where $(r_{\mathcal{F}} = 0.2, r_{\mathcal{B}} = 0), k = 0.3$, and the initial mining difficulty of $coin_{\texttt{B}}$ is 0.4. The state $(0.2, 0)$ is not a Nash equilibrium according to Theorem V.3. Because fickle miners continuously conduct the $coin_{\texttt{A}}$-mining, the mining difficulty of $coin_{\texttt{A}}$ is maintained as 1, and players in $\mathcal{M}_{\mathcal{F}}$ and $\mathcal{M}_{\mathcal{A}}$ earn the payoff of 1. If a player moves into $\mathcal{M}_{\mathcal{B}}$, the player would earn $\frac{0.3}{0.4}$ for a while in the beginning. However, because the mining difficulty of $coin_{\texttt{B}}$ decreases after $\mathcal{M}_{\mathcal{B}}$ finds several blocks, the player who moves to $\mathcal{M}_{\mathcal{B}}$ would eventually earn $\frac{0.3}{0.2}$ consistently. Note that the time duration in which the mining difficulty of $coin_{\texttt{B}}$ is close to 0 is negligible compared to the time duration in which the mining difficulty of $coin_{\texttt{B}}$ is 0.2. Therefore, the payoff of $\mathcal{M}_{\mathcal{B}}$ is $\frac{0.3}{0.2}$, and rational players tend to move to $\mathcal{M}_{\mathcal{B}}$ due to the higher payoff. This means that the state $(0.2, 0)$ is not a Nash equilibrium.

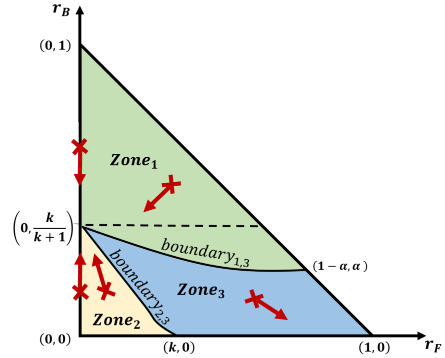

Figure 4. Horizontal and vertical axes give the values of $r_{\mathcal{F}}$ and $r_{\mathcal{B}}$, respectively, and $(r_{\mathcal{F}}, r_{\mathcal{B}})$-coordinates of vertices in zones are marked. At the vertex of $Zone_1$ and $Zone_3$, α is a solution of equation $N_{\texttt{in}} r_{\mathcal{B}}^3 + N_{\texttt{de}} r_{\mathcal{B}}(1 + k) - kN_{\texttt{de}} = 0$ for $r_{\mathcal{B}}$. All points in $Zone_1$, $Zone_2$, and $Zone_3$ move in directions $(-,-)$, $(-,+)$, and $(+,-)$, respectively.

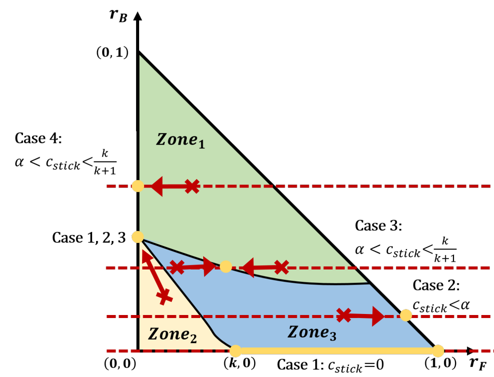

Figure 5. Yellow points and line represent equilibria for each case.

B. Dynamics in game $\mathcal{G}(\boldsymbol{c}, c_{\texttt{stick}})$

In this section, we analyze dynamics in the game $\mathcal{G}(\boldsymbol{c}, c_{\texttt{stick}})$ and study how a state can reach an equilibrium.

Best response dynamics. In game $\mathcal{G}(\boldsymbol{c}, c_{\texttt{stick}})$, point $(r_{\mathcal{F}}, r_{\mathcal{B}})$ reaches either of the two types of Nash equilibria: the stable coexistence of two coins and the lack of loyal miners to $coin_{\mathcal{B}}$. Figure 4 represents dynamics in game $\mathcal{G}(\boldsymbol{c}, c_{\texttt{stick}})$, where horizontal and vertical axes are $r_{\mathcal{F}}$ and $r_{\mathcal{B}}$ values, respectively. A line, $boundary_{1,3}$, represents

$$\frac{r_{\mathcal{B}}}{(1 - r_{\mathcal{F}} - r_{\mathcal{B}})N_{\texttt{in}} r_{\mathcal{B}}^2 + (1 - r_{\mathcal{B}})N_{\texttt{de}}(r_{\mathcal{F}} + r_{\mathcal{B}})^2} = \frac{k}{N_{\texttt{in}} r_{\mathcal{B}}^2 + N_{\texttt{de}}(r_{\mathcal{F}} + r_{\mathcal{B}})^2}. \tag{4}$$

On the line, the payoffs of $\mathcal{M}_{\mathcal{F}}$ (i.e., $U_{\mathcal{F}}(r_{\mathcal{F}}, r_{\mathcal{B}})$) and $\mathcal{M}_{\mathcal{A}}$ (i.e., $U_{\mathcal{A}}(r_{\mathcal{F}}, r_{\mathcal{B}})$) are the same. In addition, the line does not intersect with the line $(0 \le r_{\mathcal{F}} \le 1, r_{\mathcal{B}} = 0)$ and has an intersection $(1-\alpha, \alpha)$ with the line $r_{\mathcal{F}} + r_{\mathcal{B}} = 1$ for $0 \leq r_{\mathcal{F}} \leq 1$, where α is a solution of equation $N_{\mathtt{in}} r_{\mathcal{B}}^3 + N_{\mathtt{de}} r_{\mathcal{B}}(1+k) - kN_{\mathtt{de}} = 0$ for $r_{\mathcal{B}}$. The equation $N_{\mathtt{in}} r_{\mathcal{B}}^3 + N_{\mathtt{de}} r_{\mathcal{B}}(1+k) - kN_{\mathtt{de}} = 0$ has only one solution α, and it is between 0 and $\frac{k}{1+k}$. Another line, $boundary_{2,3}$, represents

$$\frac{(r_{\mathcal{F}} + r_{\mathcal{B}})}{(1 - r_{\mathcal{F}} - r_{\mathcal{B}}) N_{\mathtt{in}} r_{\mathcal{B}}^2 + (1 - r_{\mathcal{B}}) N_{\mathtt{de}} (r_{\mathcal{F}} + r_{\mathcal{B}})^2} = \frac{k}{N_{\mathtt{in}} r_{\mathcal{B}}^2 + N_{\mathtt{de}} (r_{\mathcal{F}} + r_{\mathcal{B}})^2}, \tag{5}$$

and the payoffs of $\mathcal{M}_{\mathcal{F}}$ (i.e., $U_{\mathcal{F}}$) and $\mathcal{M}_{\mathcal{B}}$ (i.e., $U_{\mathcal{B}}$) are the same on the line. The line does not intersect with the line $r_{\mathcal{F}} + r_{\mathcal{B}} = 1$ for $0 \leq r_{\mathcal{F}} \leq 1$ and has an intersection $(k, 0)$ with the line $(0 \leq r_{\mathcal{F}} \leq 1, r_{\mathcal{B}} = 0)$. Moreover, it is most profitable among the three strategies to continually conduct $coin_{\mathtt{A}}$-mining ($\mathcal{A}$) in a zone above $boundary_{1,3}$. We let this zone be $Zone_1$. In the zone below $boundary_{2,3}$, it is most profitable to continually conduct $coin_{\mathtt{B}}$-mining ($\mathcal{B}$), and the zone is denoted as $Zone_2$. In the zone between $boundary_{1,3}$ and $boundary_{2,3}$, fickle mining ($\mathcal{F}$) is the most profitable, and this zone is denoted as $Zone_3$. *Note that the range of zones changes if the coin price changes because boundaries are functions of k.*

The moving direction of point $(r_{\mathcal{F}}, r_{\mathcal{B}})$ is expressed as a red arrow in Figure 4. For ease of reading, we express directions in which values $r_{\mathcal{F}}$ and $r_{\mathcal{B}}$ increase $(+)$ or decrease $(-)$ as $(\pm, \pm)$. For example, $(+,+)$ indicates the direction in which both values, $r_{\mathcal{F}}$ and $r_{\mathcal{B}}$, increase. In $Zone_1$, $\mathcal{A}$ is the most profitable strategy, and thus every point in $Zone_1$ moves in the direction $(-,-)$. In $Zone_2$, because $\mathcal{B}$ is the most profitable strategy, every point moves in the direction $(-,+)$. Finally, in $Zone_3$, as $\mathcal{F}$ is the most profitable strategy, every point in $Zone_3$ moves in the direction $(+,-)$. Figure 4 shows the directions in the three zones ($Zone_1$, $Zone_2$, and $Zone_3$).

2D-Illustration of movement towards equilibria. To determine which equilibrium can be reached within each zone, we represent all Nash equilibria in game $\mathcal{G}(\boldsymbol{c}, c_{\mathtt{stick}})$ depending on a value of $c_{\mathtt{stick}}$ as yellow points and line in Figure 5. In the figure, the red dash lines represent $r_{\mathcal{B}} = c_{\mathtt{stick}}$ for each case. As described in Section V-A, there are two types of equilibrium points: 1) a lack of loyal miners and 2) stable coexistence of two coins. The equilibrium point representing a lack of loyal miners would be located on a red dash line $r_{\mathcal{B}} = c_{\mathtt{stick}}$, and we can see that all cases have this equilibrium. For Cases 1, 2, and 3, the second type of equilibrium (i.e., $(0, \frac{k}{k+1})$) representing stable coexistence of two coins is also found. A point $(r_{\mathcal{F}}, r_{\mathcal{B}})$ moves in the direction depending on its zone. In the meantime, if the point meets the line $r_{\mathcal{B}} = c_{\mathtt{stick}}$, then the point moves toward an equilibrium located on the line $r_{\mathcal{B}} = c_{\mathtt{stick}}$ as shown in Figure 5. In particular, the value of $r_{\mathcal{F}}$ in the equilibrium on the red dash line representing Case 3 is denoted by β, where the equilibrium is the intersection point between $boundary_{1,3}$ and the red dash line. Note, a point in $Zone_2$ would not meet a red dash line because the point in $Zone_2$ moves in the direction $(-,+)$ and can always be above the red dash line. Therefore, such points in $Zone_2$ are likely to reach the stable coexistence of $coin_{\mathtt{A}}$ and $coin_{\mathtt{B}}$. However, some points (near to $boundary_{2,3}$) in $Zone_2$ can also move into $Zone_3$ when more miners of $\mathcal{M}_{\mathcal{A}}$ than that of $\mathcal{M}_{\mathcal{F}}$ revise their strategies, and then it is possible to reach the equilibrium, representing a lack of loyal miners to $coin_{\mathtt{B}}$.

VI. Application to Bitcoin System

In this section, we apply our game model to Bitcoin as a case study. Specifically, we consider game $\mathcal{G}(\boldsymbol{c}, c_{\mathtt{stick}})$ when players possess sufficiently small mining power. To see if this assumption is reasonable, we investigate the mining power distribution in the Bitcoin system, referring to the power distribution provided by Slush [32]. The distribution is depicted in Figure 6 where the x-axis represents the range of the relative computational power c_i and the y-axis represents the number of miners possessing computational power in the corresponding range. The figure shows that 1) most miners possess sufficiently small mining power, and 2) even the maximum computational power is less than 10^{-2}. Note that BITMAIN's c_i is about $3 \cdot 10^{-2}$ as of Dec. 2018. Moreover, even though mining pools currently possess large computational power, the miners in pools can individually decide which coin to mine. We also recognize the distribution of computational power is significantly biased toward a few miners, as shown in Figure 6. However, this fact does not imply that $\|\boldsymbol{c}\|_2$ is large. Referring to the data provided by Slush, $\|\boldsymbol{c}\|_2$ is only about 0.05, where this value is equivalent to that for the case where all miners possess 2.5×10^{-3} computational power.[2] Therefore, most miners (and most mining power) would follow dynamics of game $\mathcal{G}(\boldsymbol{c}, c_{\mathtt{stick}})$. As a result, we can apply game $\mathcal{G}(\boldsymbol{c}, c_{\mathtt{stick}})$ to the practical systems.

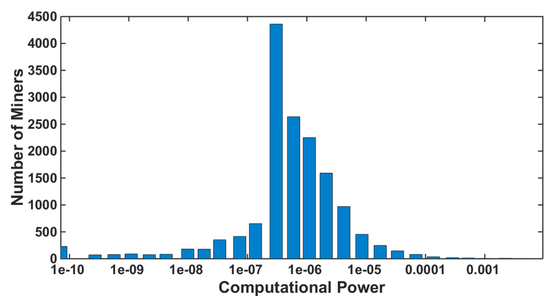

Figure 6. The computational power distribution in Slush.

Now, we describe how game $\mathcal{G}(\boldsymbol{c}, c_{\mathtt{stick}})$ is applied to the Bitcoin system. As described in Section II, Bitcoin was split into BTC and BCH in Aug. 2017. Thus, we can map BTC and BCH to $coin_{\mathtt{A}}$ and $coin_{\mathtt{B}}$, respectively. For the mining difficulty adjustment algorithm of BCH, we should consider two types of BCH mining difficulty adjustment algorithms: those that BCH have before and after Nov. 13, 2017. This is

[2]We calculated this assuming that other pools have the computational power distribution similar to Slush.

because the mining difficulty adjustment algorithm of BCH changed through a hard fork of BCH (on Nov. 13, 2017).

Before Nov. 13, 2017. First, we consider the mining difficulty adjustment algorithm of BCH before Nov. 13, 2017. In this algorithm, not only the mining difficulty is adjusted for every 2016 block, but also EDA can occur as described in Section II. Note that EDA occurs if the mining is significantly difficult in comparison with the current mining power, i.e., EDA is used only for *decreasing* the BCH mining difficulty. Therefore, the value of $N_{\mathtt{in}}$ is 2016 because the BCH mining difficulty can increase after 2016 blocks are found. Meanwhile, when the BCH mining difficulty decreases, the value of $N_{\mathtt{de}}$ varies depending on $r_{\mathcal{F}}$ and $r_{\mathcal{B}}$, ranging between 6 and 2016. Thus, we can consider the expected number of blocks found until the mining difficulty decreases (i.e, the mean of $N_{\mathtt{de}}$ denoted by $E[N_{\mathtt{de}}]$) instead of $N_{\mathtt{de}}$, and $E[N_{\mathtt{de}}]$ as a function of $r_{\mathcal{F}}$ and $r_{\mathcal{B}}$ would continuously vary from 6 to 2016. If $r_{\mathcal{F}}$ is 0, $E[N_{\mathtt{de}}]$ is 2016 because EDA does not occur, and if $r_{\mathcal{B}}$ is 0, $E[N_{\mathtt{de}}]$ is 6.

As a result, the Bitcoin system before Nov. 13, 2017 can be $\mathcal{G}(\boldsymbol{c}, c_{\mathtt{stick}})$ where $E[N_{\mathtt{de}}]$ substitutes for $N_{\mathtt{de}}$. This game $\mathcal{G}(\boldsymbol{c}, c_{\mathtt{stick}})$ has also Nash equilibria and dynamics as shown in Figure 4 because $E[N_{\mathtt{de}}]$ is a continuous function of $r_{\mathcal{F}}$ and $r_{\mathcal{B}}$.

After Nov. 13, 2017. Next, we consider the Bitcoin system after Nov. 13, 2017. In this case, the BCH mining difficulty adjustment algorithm is different from that assumed in our game because the mining difficulty is adjusted for every block by considering the generation time of the past 144 blocks as a moving time window. Despite that, game $\mathcal{G}(\boldsymbol{c}, c_{\mathtt{stick}})$ can be applied to this system. Indeed, in general, our results for game $\mathcal{G}(\boldsymbol{c}, c_{\mathtt{stick}})$ would appear in the Bitcoin system regardless of the BCH mining difficulty adjustment algorithm, shown below.

Theorem VI.1. *Consider the game $\mathcal{G}(\boldsymbol{c}, c_{\mathtt{stick}})$ when $\|\boldsymbol{c}\|_2 \approx 0$. Then when the mining difficulty of coin$_{\mathtt{B}}$ is adjusted every block or in a short time period, the set $\mathcal{E}(\boldsymbol{c}, c_{\mathtt{stick}})$ is* (3) *presented in Theorem V.3. In addition, $\mathcal{G}(\boldsymbol{c}, c_{\mathtt{stick}})$ under this mining difficulty adjustment algorithm of coin$_{\mathtt{B}}$ has dynamics such as in Figure 4.*

Because the current BCH mining difficulty is adjusted every block, Theorem VI.1 implies that results for game $\mathcal{G}(\boldsymbol{c}, c_{\mathtt{stick}})$ is also applied to the current Bitcoin system even though the BCH mining difficulty adjustment algorithm changed. The proof of Theorem VI.1 is presented in the full version of this paper [31].

VII. Data analysis

A. BTC vs. BCH

We analyze the mining power data in the Bitcoin system to identify to which equilibrium the state has been moving. Moreover, through this data analysis, we can find out empirically how much our theoretical model agrees with practical results. For data analysis of the Bitcoin system, we collected the mining power data of BTC and BCH from the release date of BCH (Aug. 1, 2017) until the time of writing (Dec. 10, 2018) from CoinWarz [33]. Figure 7a represents the mining power history of BCH, where the mining power is expressed as a fraction of the total power in BTC and BCH, i.e.,

$$\frac{\text{BCH mining power}}{\text{BTC mining power} + \text{BCH mining power}}.$$

In addition, we represent the data history of a ratio between difficulties of BCH and BTC (i.e., $\frac{D_{\mathtt{B}}}{D_{\mathtt{A}}}$) and a relative price of BCH to that for BTC (i.e., k) in Figure 7b and 7c, respectively. The price of BCH is depicted as a yellow line in Figure 7c (see the left y-axis). Moreover, Figure 7c represents the relative BCH mining profitability ($\frac{kD_{\mathtt{A}}}{D_{\mathtt{B}}} - 1$) to the BTC mining profitability as a purple line, and the black dashed line represents $\frac{kD_{\mathtt{A}}}{D_{\mathtt{B}}} - 1 = 0$ (see the right y-axis for the two lines). For this profitability, to increase reliability of data, we collected the daily BCH profitability from CoinDance [34], and thus a purple point is a data captured every day. Note that $\frac{D_{\mathtt{B}}}{D_{\mathtt{A}}}$ is less than k in the case where the purple line is above the black dashed line. Figure 7d simultaneously shows all data histories (except for the BCH mining profitability) presented in Figure 7a∼7c. In Figure 7, the data from Dec. 2017 to Nov. 2018 are omitted because they are similar to the data for Dec. 2018. Figure 8a∼8i correspond to parts (1)∼(9) of Figure 7, respectively, where the area of three zones has changed because the relative price k of BCH to that for BTC has fluctuated quite frequently.

As another case study, we examine the mining power data of Bitcoin ABC and Bitcoin SV from Nov. 1, 2018 to Dec. 20, 2018 to analyze a special situation where $c_{\mathtt{stick}}$ suddenly increases due to the "hash war" caused by a hard fork in the BCH system. We describe this in Section VII-B.

Methodology. We first describe how to determine $r_{\mathcal{F}}$ and $r_{\mathcal{B}}$ of each state. According to the definition of fickle mining (Definition IV.1), fickle miners would conduct BCH mining from when $\frac{D_{\mathtt{B}}}{D_{\mathtt{A}}}$ *changes* to a value less than k to when $\frac{D_{\mathtt{B}}}{D_{\mathtt{A}}}$ *changes* to a value greater than k. This is because $D_{\mathtt{B}}$ is always less than $r_{\mathcal{F}} + r_{\mathcal{B}}$ and greater than $r_{\mathcal{B}}$ (see Figure 7d). Therefore, Figure 7a represents the value of $r_{\mathcal{F}} + r_{\mathcal{B}}$ during the period. We indicate the fickle mining periods in gray before the hard fork of BCH (Nov. 13, 2017) in Figure 7. Figure 7d shows that $\frac{D_{\mathtt{B}}}{D_{\mathtt{A}}}$ changes to a value less than and greater than k at the start and end of these periods, respectively. As a result, in Figure 7a, we can find out the value of $r_{\mathcal{F}} + r_{\mathcal{B}}$ for the gray colored periods and the value of $r_{\mathcal{B}}$ for non-colored periods. Here, we can see that the mining power of BCH has fluctuated considerably when the ratio of the BCH mining difficulty to the BTC mining difficulty ($\frac{D_{\mathtt{B}}}{D_{\mathtt{A}}}$) *changes* to a value less than k. Moreover, when the coin mining difficulties do not change while BCH mining is more profitable than BTC mining, large *peaks* (i.e., a sudden increase) do not appear. This fact is confirmed, referring to the purple line in non-colored zones (e.g., part (3) in Figure 7c). As a result, we can consider that those fluctuations occur due to fickle miners between BTC and BCH.

If a miner switches the coin to mine without changes in the coin mining difficulty, this implies that the miner's strategy

(a)

(b)

(c)

(d)

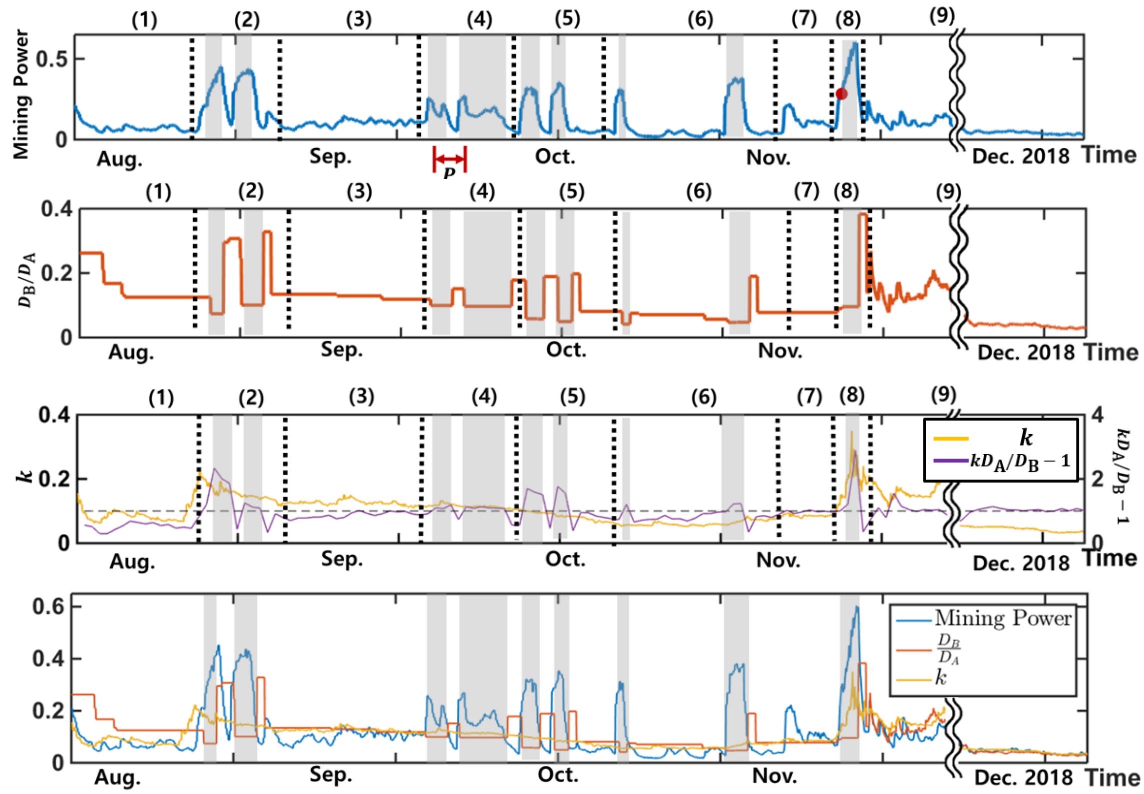

Figure 7. The data for the Bitcoin system from early Aug. 2017 to Dec. 2018 is represented. Figure 7a, 7b, and 7c represent (a) relative mining power of BCH to the total mining power, (b) the ratio between mining difficulties of BCH and BTC, (c) the ratio between prices of BCH and BTC, and BCH mining profitability. Figure 7d shows the data for mining power, price, and mining difficulty of BCH. In the gray zones, fickle miners conduct BCH mining. The data from Dec. 2017 to Nov. 2018 are omitted because they are similar to the data for Dec. 2018. Each point represents a data captured every hour.

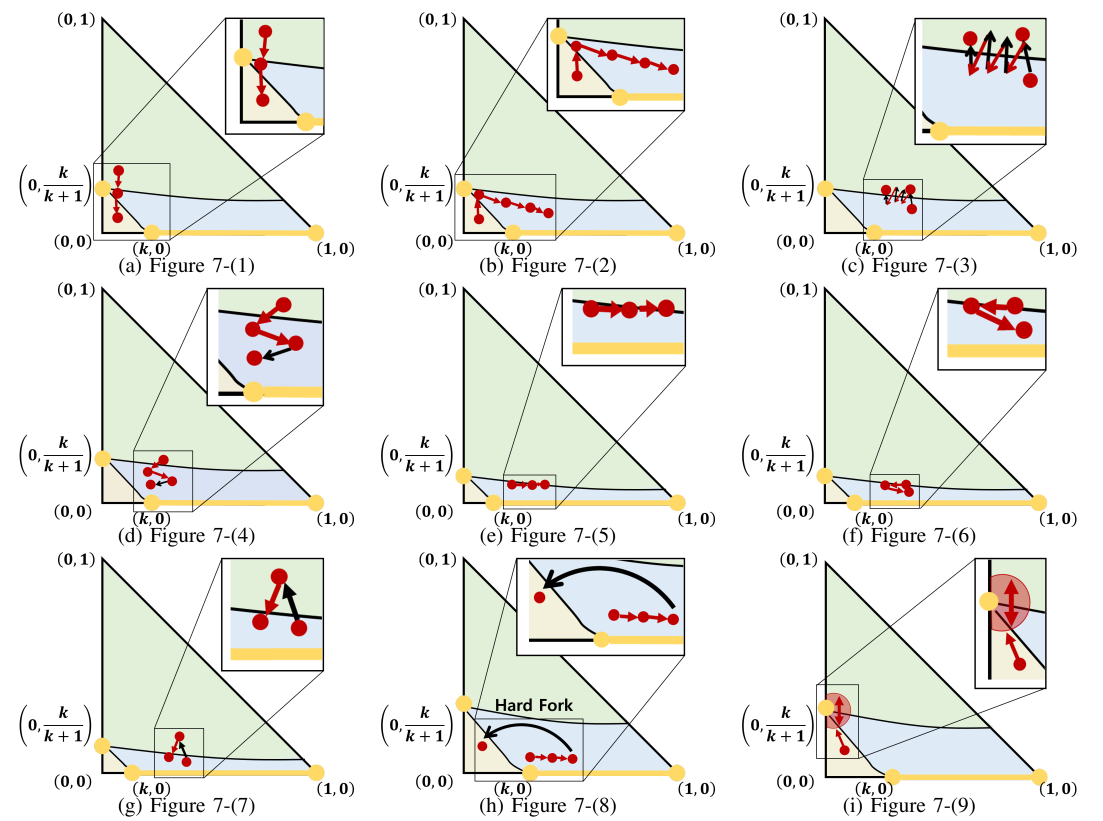

Figure 8. Points and movements of Figure 7. Figure 8a ∼ 8i correspond to parts (1)∼(9) in Figure 7. Red arrows represent movement in agreement with our model, whereas black arrows represent movement deviating from our model. Each upper right square presents enlarged points and directions.

changes (e.g., from $\mathcal{A}$ to $\mathcal{B}$). From the method described above, we can determine the mining power $r_{\mathcal{F}}$ used for fickle mining and the mining power $r_{\mathcal{B}}$ used for BCH-only mining. The points and directions are marked roughly in Figure 8. The red arrow represents movement in agreement with our analysis, whereas the black arrow represents movement deviating from our analysis.

Next, we explain Figure 8 by matching it with each part of Figure 7.

The beginning of the game. In Figure 7-(1), the status point is initially in $Zone_1$, and then it moves to $Zone_2$ as shown in Figure 8a, as the BCH mining power decreases.

Towards the lack of BCH loyal miners. In Figure 7a-(2), two peaks occur when the BCH mining difficulty decreases to values less than k, and these peaks appear in the gray colored periods. Therefore, we can know that these peaks occur due to fickle miners. The first peak indicates that more and more miners started fickle mining (i.e., increase in $r_{\mathcal{F}}$). This is because the upflow of the first peak is less steep than that for other peaks, and the downflow of the first peak is steeper than the upflow of the first peak, indicating that $r_{\mathcal{F}}$ increases from near 0 up to near 0.4. Furthermore, one can see that $r_{\mathcal{B}}$ increased at the beginning of Figure 7a-(2). Remark that Figure 7a shows the value of $r_{\mathcal{B}}$ in a non-colored zone. In addition, the BCH mining power in the valley between two peaks of Figure 7a-(2) is greater than the mining power at the end of Figure 7a-(1). This fact shows again that $r_{\mathcal{B}}$ increased at the beginning of Figure 7a-(2). After that, because the end of Figure 7a-(2) is less than the valley between the two peaks of Figure 7a-(2), we can know that $r_{\mathcal{B}}$ decreased while $r_{\mathcal{F}}$ increased in Figure 7a-(2). Figure 8b represents these movements described above.

In the beginning of Figure 7a-(3), $r_{\mathcal{B}}$ slightly increases, and it does not correspond with our model; we regard this as a momentary phenomenon because of a decrease in the BCH mining difficulty. Figure 7b shows that the BCH mining difficulty decreased at the beginning of the part (3). However, even though the BCH mining difficulty decreased, peaks due to fickle mining do not appear because the relative BCH mining difficulty did not decrease to a value less than k as shown in Figure 7d. As a result, as can be seen in Figure 8c, the point moves alternatively between $Zone_1$ and $Zone_3$. One can see that $r_{\mathcal{F}}$ decreased compared with the mining power in the peaks of Figure 7a-(4) and the peaks in Figure 7a-(2); this might be because the moving direction in $Zone_1$ is $(-,-)$.

Next, the peaks in the period P presented in Figure 7a-(4) appeared due to fickle miners because the BTC mining difficulty increased. We can check that $\frac{D_{\mathtt{B}}}{D_{\mathtt{A}}}$ in the period P decreased to a value less than k through Figure 7d. Note that the fact that the BTC mining difficulty increased makes the value of $\frac{D_{\mathtt{B}}}{D_{\mathtt{A}}}$ decrease. Indeed, the two peaks of the period P show that $r_{\mathcal{F}}$ decreases and then increases because $r_{\mathcal{F}} + r_{\mathcal{B}}$ is represented in the period P of Figure 7a. This may be explained according to our model as follows: the state was near to the boundary between $Zone_1$ and $Zone_3$ at the beginning of Figure 7-(4), and then the state entered $Zone_3$ while moving in the direction $(-,-)$ (the moving direction in $Zone_1$) as in Figure 8d. Then, the state in $Zone_3$ moved in the direction $(+,-)$ in agreement with our game, and one can see that the third peak (i.e., the beginning of the second gray colored zone in Figure 7a-(4)) is higher than the second peak. After that, $r_{\mathcal{F}}$ decreases (see the second gray colored zone in Figure 7a-(4)), showing a deviation from our model, which is indicated by the black arrow in Figure 8d. Indeed, considering this case as well as Figure 7-(3), we observe such noises in the case where $\frac{D_{\mathtt{B}}}{D_{\mathtt{A}}}$ changes to a value close to k.

Next, as shown in Figure 8e, the point in $Zone_3$ moves in the direction $(+,-)$ again because peaks in Figure 7a-(5) are higher than that for Figure 7a-(4). Moreover, in Figure 7c-(4)∼(6), k is roughly decreasing and even drops to about 0.055 in a few cases. In the meantime, the point passes $boundary_{1,3}$.

Because the state entered $Zone_1$, $r_{\mathcal{F}}$ starts to decrease, moving in the direction $(-,-)$ (as shown in Figure 8f). Therefore, the first peak in Figure 7a-(6) is smaller than the last peak in Figure 7a-(5). Then, because the second peak is higher than the first peak in Figure 7a-(6), one can see that the point moved in the direction $(+,-)$ in $Zone_3$ in agreement with our model, which is, in turn, depicted in Figure 8f.

As can be seen in Figure 8g, $r_{\mathcal{B}}$ first increases in Figure 7a-(7), and the point enters $Zone_1$; this is a deviation from our analysis, which may be explained because the BCH mining is momentarily more profitable than the BTC mining at the time. Here, we can see again the noise in the case where the value of $\frac{D_{\mathtt{B}}}{D_{\mathtt{A}}}$ is close to k. However, $r_{\mathcal{B}}$ decreases again in agreement with our model. In addition, one can see that $r_{\mathcal{F}}$ decreases in the meantime because the starting height of the peak in Figure 7a-(8), which is marked by a red point, is less than that of the final peak in Figure 7a-(6). Therefore, the point in $Zone_1$ moved in the direction $(-,-)$ and entered $Zone_3$, conforming with our analysis.

Then, in the second week of Nov. 2017, the price of BCH was suddenly pumped ($k \approx 0.4$ in some cases). Therefore, $Zone_2$ widens in Figure 8h. Also, the point in $Zone_3$ continuously moves in the direction $(+,-)$, and $r_{\mathcal{F}}$ even increases to over 0.5. It can be seen that the peak in Figure 7-(8) has a right-angle trapezoid with a positive slope, which indicates that $r_{\mathcal{F}}$ continuously increases even though it was *already* high. From the history, we observe that the Bitcoin system often reaches the lack of BCH loyal miners. However, a breakthrough exists even in this bad situation. If k continuously increases, $Zone_2$ widens, and it makes the state enter $Zone_2$ and reach close to the coexistence equilibrium. As a result, considering the state of Bitcoin as of Nov. 13, 2017, k had to increase to a minimum of 0.5 in order for the mining power engaging in fickle mining to decrease.

Close to coexistence. However, at the end of Figure 7-(8), another hard fork occurred in BCH for updating the difficulty adjustment algorithm, and this influenced the status as an external factor. Consequently, the point jumped into $Zone_2$ due to this hard fork as shown in Figure 8h. After the hard fork, the point moves in the direction $(-,+)$, reaching close to coexistence. This is shown by this fact that fluctuations became stable more and more in the beginning of Figure 7a-(9). Note that peaks occur in a short time after the hard fork because the BCH mining difficulty is quickly adjusted. Even though the state has been close to coexistence, fickle mining is still possible and observed as described in Section II. In addition, as the price continuously changes, the point sometimes enters $Zone_3$ where fickle mining increases, alternating up and down in the red semicircle in Figure 8i. In other words, fickle mining will not completely cease. Therefore, if the Bitcoin state largely deviates from the equilibrium of coexistence due to external factors such as a *sudden* change in prices, then it is still possible to reach the lack of BCH loyal miners.

Influence of the lack of BCH loyal miners. We observe that the Bitcoin system suffered from the lack of BCH loyal miners before Nov. 13, 2017. Consequently, the BCH transaction process speed periodically became low, and it even took about four hours to generate one block in some cases. Moreover, we can see that BCH was significantly centralized during the period in which the BCH mining difficulty is high. For example, when considering blocks generated from Oct. 2 to Oct. 4, only two accounts generated about 70 % of blocks and there were only five miners who conducted BCH mining. We note that, in blockchain systems using a PoW mechanism, high mining power is an essential factor for high security blockchain systems. In practice, BCH before Nov. 13, 2017 was susceptible to double spending attacks with only 1∼2% of the total computational power in the Bitcoin system. There is also selfish mining [15], which makes the attacker unfairly earn the extra reward while others suffer a loss. Because of a decrease in $r_{\mathcal{B}}$, these attacks can be executed with relatively small mining power. As a result, fickle mining, which heavily occurred before Nov. 13, 2017, weakened the performance, decentralization level, and security of the BCH system.

Influence of the hard fork of BCH. Next, we discuss why Bitcoin moved toward different equilibria before and after Nov. 13, 2017. First, in the Bitcoin system before Nov. 13, 2017, $r_{\mathcal{F}}$ considerably increased as can be seen in Figure 7a-(2). Meanwhile, after Nov. 13, 2017, $r_{\mathcal{F}}$ did not considerably increase even though the point passed $Zone_3$. This can be attributed to the different difficulty adjustment algorithms before and after Nov. 13, 2017; the mining difficulty of BCH is currently adjusted faster than that before Nov. 13, 2017. Therefore, currently, to conduct fickle mining, miners must switch between BTC and BCH relatively fast; this would make the current fickle mining in the Bitcoin system annoying. Then, can we regard the current state of BCH to be safe if the system avoids external factors such as a *sudden* change in prices? We delay the answer until Section VIII.

B. The "hash war" between Bitcoin ABC and Bitcoin SV

According to our model, we also describe the "hash war" that recently occurred between Bitcoin ABC (ABC) and Bitcoin SV (BSV), which are derived from the original BCH on Nov. 15, 2018. In this paper, we call 'Bitcoin ABC' ABC rather than BCH to avoid confusion with the original BCH even though Bitcoin ABC is currently regarded as BCH [35]. This war was caused by the conflict over a BCH update that adds a new *opcode*, where the BCH factions split into a reformist group and an opposing group. As a result, this conflict caused the two factions to make their own chain, where the reformist group is the ABC faction led by Roger Ver (the owner of *Bitcoin.com* [36]) and Jihan Wu (the cofounder of Bitmain and also the owner of BTC.com [9] and Antpool [37]) and the opposing group is the BSV faction led by Craig Wright and Calvin Ayre (the CEO of Coingeek [38]). This split of the original BCH was achieved by a hard fork on Nov. 15, 2018, and each faction wanted its own chain to be the longest chain in order to unify the divided BCH. This fact makes both factions desperately conduct mining of their coins with vast computational power; thus the hash war occurred from Nov. 15, 2018 to Nov. 24, 2018. Such behavior of ABC and BSV factions would influence on a general miner who choose its coin among BTC, ABC, and BSV, and we analyze this situation by dividing into two games: 1) a game between BTC and ABC and 2) another game between BTC and BSV. In both games, $c_{\texttt{stick}}$ became significantly high during the hash war period, and we can consider this situation as Case 4 ($c_{\texttt{stick}} > \frac{k}{k+1}$).

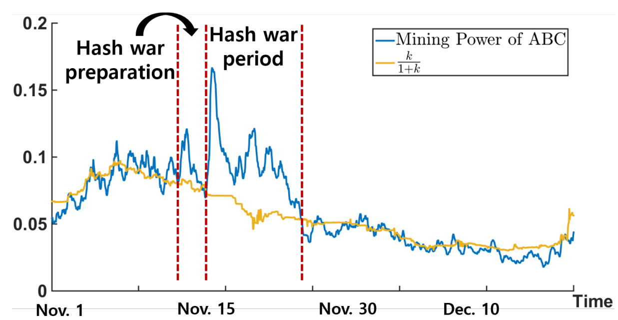

Figure 9. The data for ABC from **Nov. 1, 2018** to Dec. 20 2018 is represented. The mining power of ABC is expressed as a relative value to the total power in BTC and ABC, and k indicates a relative price of ABC to that for BTC.

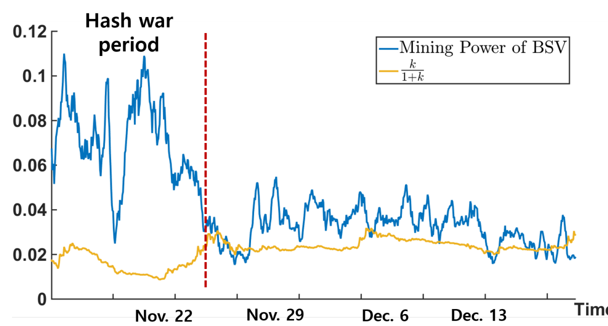

Figure 10. The data for BSV from **Nov. 15, 2018** to Dec. 20 2018 is represented. In this figure, mining power of BSV is expressed as a relative value to the total power in BTC and BSV, and k indicates a relative price of BSV to that for BTC.

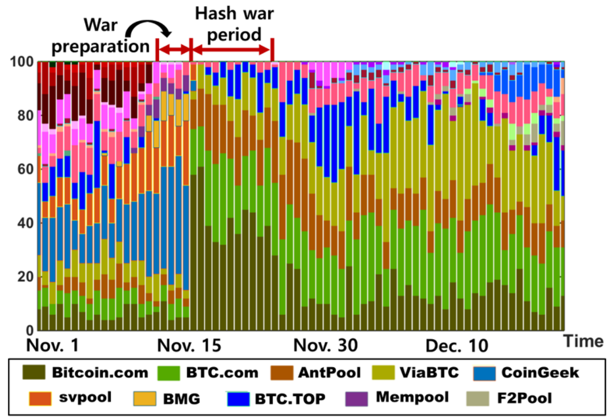

Figure 11. The x and y-axes represent time from **Nov. 1, 2018** to Dec. 20, 2018 and the number of ABC blocks generated by each miner in previous 100 blocks, respectively. The name of a miner corresponding to each color is presented at the bottom of this figure.

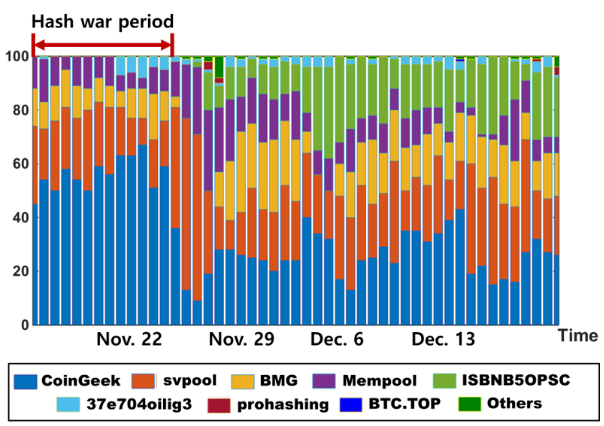

Figure 12. The x and y-axes represent time from **Nov. 15, 2018** to Dec. 20, 2018 and the number of BSV blocks generated by each miner in previous 100 blocks, respectively. The name of a miner corresponding to each color is presented at the bottom of this figure.

To analyze a phenomenon that appeared due to the hash war, we collect the data for ABC and BSV. Figure 9 and 10 show the ABC data history from Nov. 1, 2018 to Dec. 20, 2018 and the BSV data history from Nov. 15, 2018 to Dec. 20, 2018, respectively. Note that BSV was released on Nov. 15, 2018. In Figure 9, the mining power of ABC is presented as a relative value to the total mining power of ABC and BTC, and $\frac{k}{k+1}$ is also presented, where k indicates a relative price of ABC to that for BTC. Figure 10 depicts the data history of BSV like Figure 9. These figures show that the state $(r_{\mathcal{F}}, r_{\mathcal{B}})$ in the two games was above the state $(0, \frac{k}{1+k})$ during the hash war period.

Moreover, to determine the movement of the state for the hash war period, we investigate the history of ABC computational power distribution among miners from Nov. 1, 2018 to Dec. 20, 2018 and that for BSV from Nov. 15, 2018 to Dec. 20, 2018. This is because it would be hard to determine the movement of the state through just the mining power history (i.e., Figure 9 and 10) because $c_{\texttt{stick}}$ significantly changed during this period. Figure 11 and 12 represent the changes in the mining power distribution of ABC and BSV over time, respectively. To do this, we crawled coinbase transactions and analyzed the number of blocks mined by each miner among previous 100 blocks. In these figures, each miner corresponds to one color, and the length of one colored bar represents the number of blocks generated by the corresponding miner among 100 blocks. Therefore, the number of colors in the entire bar indicates the number of active miners at the corresponding time. Note that only names of ten miners are presented in Figure 11.

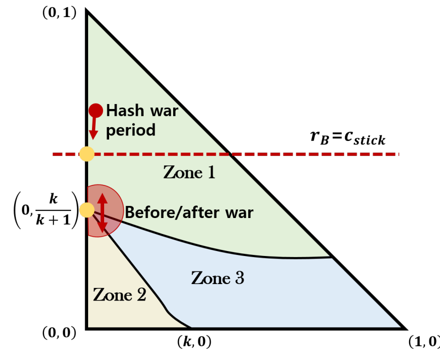

Figure 13. This figure describes the movement of state for hash war period and the movement of state before and after war.

First, we consider the game between BTC and ABC. One can see that the state $(r_{\mathcal{F}}, r_{\mathcal{B}})$ jumps to a point above $(\frac{k}{k+1}, 0)$ for the hash war preparation period (from Nov. 13, 2018 to Nov.15, 2018) through Figure 9. Such an increase in the ABC mining power may be explained because the mining power of BSV factions such as CoinGeek, svpool, BMG pool, and Mempool increased from the hash war preparation [39] as shown in Figure 11. In other words, the increase in the ABC mining power for the hash war preparation is because $c_{\texttt{stick}}$ increased. On the other hand, Figure 11 shows that some miners left the ABC system during the war preparation (the colors that appeared at the top of the figure before the war preparation period disappeared from the war preparation period). This fact indicates that the state moves toward the line $r_{\mathcal{B}} = c_{\texttt{stick}}$ in the case that $c_{\texttt{stick}}$ is large. Note that the reason why the ABC mining power decreases at the end of the hash war preparation period (i.e., the start of the hash war) is that BSV factions move to the BSV system.

Next, for the hash war period, the ABC mining power increased because the ABC factions such as Bitcoin.com increased their mining power (i.e., $c_{\texttt{stick}}$ increased) [35]. However, there were only a few loyal ABC miners during this period. For example, at the start of the hash war, only five miners exist: Bitcoin.com, BTC.com, AntPool, ViaBTC, and BTC.TOP. Note that all of them are the ABC factions (ViaBTC and BTC.TOP announced that they support ABC [40], [41]). As a result, we can see that this state is close to the state $r_{\mathcal{B}} = c_{\texttt{stick}}$, which represents a lack of BCH loyal miners. This state makes the ABC system severely centralized. In particular, one miner (Bitcoin.com) possessed about 60 % of the total computational power in some cases, which indicates the breakage of censorship resistance. Meanwhile, after the hash war (i.e., when $c_{\texttt{stick}}$ is less than $\frac{k}{k+1}$), one can see that more other miners gradually enter the ABC system (see the increase in the number of colors after the hash war in Figure 11). In addition, Figure 9 shows that the state is close to $\frac{k}{k+1}$ after the hash war. As a result, the state moves as shown in Figure 13.

Second, we describe the game between BTC and BSV through Figure 10 and 12. As shown in Figure 10, the state is above $(0, \frac{k}{k+1})$ for the hash war period because $c_{\texttt{stick}}$ is significantly high. This fact is also presented in Figure 12. Note that CoinGeek, svpool, BMG, and Mempool are BSV factions. Therefore, the state was close to $r_{\mathcal{B}} = c_{\texttt{stick}}$ at the time. Similar to ABC, BSV also suffered from the severe centralization due to a lack of loyal miners. However, the other miners have entered the BSV system after the hash war, and the state became close to $(0, \frac{k}{k+1})$. Therefore, Figure 13 represents the state movement, and this result empirically confirms our theoretical analysis.

Here, note that when the state is located above $\frac{k}{k+1}$, $\Omega_{\texttt{stick}}$ suffers a loss. This fact makes the state $c_{\texttt{stick}} > \frac{k}{k+1}$ would not last for a long time. Therefore, the hash war was also not able to continue for a long time, and the hash war ended with BSV's surrender [42].

VIII. Broader Implications

In this section, we describe broader implications of our game model. More precisely, we first describe the risk of automatic mining, and then explain how one coin can exploit this risk to *intentionally* steal the loyal miners from other less valued coins with negligible efforts and resources.

A. A potential risk of automatic mining

As described above, the current state of Bitcoin is close to coexistence between BTC and BCH because faster BCH mining difficulty adjustment makes *manual* fickle mining inconvenient. We introduce another possible mining scheme called *automatic mining*, which can be less affected by faster mining difficulty adjustment. Automatic mining is designed for miners to automatically switch the coin to mine to the likely most profitable one of the compatible coins by analyzing their mining difficulty and coin prices in real time unlike fickle mining. Here, note that all automatic miners almost *simultaneously* change their coin when not only mining difficulty but also coin prices changes. Indeed, automatic mining can be considered to be automatically choosing the most profitable one among three strategies, $\mathcal{F}$, $\mathcal{A}$, and $\mathcal{B}$ in real time. Automatic mining has been executed in the Bitcoin system [43] and has already become popular in the altcoin system [44]. Indeed, mining power increases and decreases by more than a factor of four in most altcoins several times a day [45]. We describe a simple implementation of automatic mining below.

Currently, many mining pools, including BTC.com, Antpool, and ViaBTC, support interactive user interfaces for

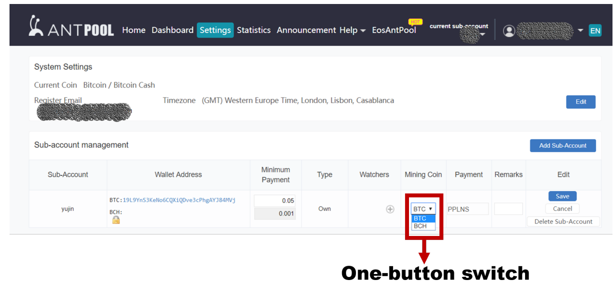

Figure 14. One-button switching mining in Antpool

switching the coin to mine by just clicking one button. Figure 14 represents the one-button switching mining feature provided by Antpool. This feature makes automatic mining easier without technical difficulties in implementing this approach. For example, a miner can conduct automatic mining in Antpool as follows.

1) First, the miner saves an HTTP header with its cookies to maintain the login session.
2) To determine which coin is more profitable, the miner calculates the mining profitability of BTC and BCH. In real-world settings, this can be simply implemented by using real-time coin prices [46], [47] and the coin mining difficulty.
3) If BTC mining is more profitable than BCH mining, the miner sends an HTTP request, which includes the saved HTTP header and data for switching to BTC mining. Otherwise, the miner sends an HTTP request to conduct BCH mining.
4) The above steps are repeated.

As shown in the code [48], this automatic mining can be executed within about 50 lines in Python.

Large-scale automatic mining makes the state of the coin system enter $Zone_3$. As a simple example, we can consider an extreme case wherein the entire computational power is involved in automatic mining. In this case, any initial state except for $(0, \frac{k}{k+1})$ immediately reaches the equilibrium $r_{\mathcal{B}} = c_{\texttt{stick}}$ as soon as all miners start automatic mining. This is because all automatic miners should simultaneously choose the same coin and would eventually mine $coin_{\texttt{A}}$ when the mining difficulty of $coin_{\texttt{B}}$ increases.

Then, we have the following question: What ratio of automatic mining power is needed to reach the lack of $coin_{\texttt{B}}$-loyal miners? As shown in Figure 4, the state $(r_{\mathcal{F}}, r_{\mathcal{B}})$ cannot be in $Zone_2$ when $r_{\mathcal{F}}$ is not less than k. Therefore, $(r_{\mathcal{F}}, r_{\mathcal{B}})$ where $r_{\mathcal{F}} \geq k$ would move in the decreasing direction of $r_{\mathcal{B}}$. Further, even manual miners who do not conduct automatic mining would prefer $coin_{\texttt{A}}$ rather than $coin_{\texttt{B}}$ at states in $Zone_3$ where $r_{\mathcal{F}} \geq k$ because $coin_{\texttt{A}}$-only mining is more profitable than $coin_{\texttt{B}}$-only mining at the states; loyal miners of $coin_{\texttt{B}}$ should generate blocks with high difficulty. Therefore, when a fraction k of the total mining power is involved in the automatic fickle mining, the state moves towards a lack of $coin_{\texttt{B}}$-loyal miners. As of Dec. 2018, because k in the Bitcoin system is about 0.05, if 5% of the total mining power in the Bitcoin system is involved in automatic mining, the automatic miners would conduct (automatic) fickle mining and the state would enters $Zone_3$. Note that if automatic miners of which the total mining power is 5% conduct $coin_{\mathtt{A}}$-only (or $coin_{\mathtt{B}}$-only) mining, the state would enter $Zone_2$ (or $Zone_1$). This is contradiction because the automatic miners should choose the most profitable strategy. As a result, when only 5% of the total mining power is involved in the automatic mining, the number of BCH loyal miners decreases and the BCH system is finally becoming more centralized.

B. Injuring rivalry coins

In Section VI, we explained how our game $\mathcal{G}(\boldsymbol{c}, c_{\mathtt{stick}})$ can be applied to the Bitcoin system regardless of the BCH mining difficulty adjustment algorithm. To generalize our game model, we here consider two types of possible mining difficulty adjustment algorithms: The first type of algorithm is to adjust the mining difficulty in a long time period (e.g., two weeks) while the second type of algorithm is to adjust the mining difficulty every block or in a short time period in order to promptly respond to the changes in the mining power. In the real-world, both types of these mining difficulty adjustment algorithms are mostly used. For example, BTC and Litecoin are the cryptocurrency systems using the first type, while many altcoins including BCH, Ethereum (ETH), and Ethereum Classic (ETC) are currently using the second type.

We can generalize our game model to any coin system satisfying the following conditions.

1) Two existing coins share the same mining hardware.
2) The more valued coin $coin_{\mathtt{A}}$ between those coins has the first type of mining difficulty adjustment algorithm.

We note that there is no restriction on the mining difficulty adjustment algorithm for the less valued $coin_{\mathtt{B}}$ in our game model $\mathcal{G}_\infty$. When $coin_B$ has the first type of mining difficulty adjustment algorithm, our model can be applied according to Section IV. Note that we modeled our game in Section IV, assuming that $coin_B$ has the first type of mining difficulty adjustment algorithm. In addition, in Section VI, we described why our game can be applied to when $coin_B$ has the second type of mining difficulty adjustment algorithm. Therefore, regardless of $coin_{\mathtt{B}}$ mining difficulty adjustment algorithm, in the coin system satisfying the above two conditions, the $coin_{\mathtt{B}}$-loyal miners would leave if at least k fraction of the total mining power is involved in automatic mining.

Next, we explain how the more valued coin can steal loyal miners from the other less valued rivalry coin. If $coin_{\mathtt{A}}$ utilizes the first type of mining difficulty adjustment algorithm, the number of $coin_{\mathtt{B}}$-loyal miners would naturally decrease due to the automatic mining. Again note that this situation periodically weakens the health of the $coin_{\mathtt{B}}$ system in terms of security and decentralization. On one hand, if $coin_{\mathtt{A}}$ has a mining difficulty adjustment algorithm different from the first type (i.e., different from that in Assumption 3), our game model may not be applied. For example, when considering the Ethereum system consisting of ETH and ETC, ETH corresponding to $coin_{\mathtt{A}}$ has a different difficulty adjustment algorithm from that which we assumed in our game. In this case, even if $r_{\mathcal{B}} = 0$, the complete downfall of $coin_{\mathtt{B}}$ (e.g., ETC) may not occur and the mining power of $coin_{\mathtt{A}}$ and $coin_{\mathtt{B}}$ would fluctuate heavily. Therefore, to follow our game and so steal the loyal miners from $coin_{\mathtt{B}}$, $coin_{\mathtt{A}}$ should change its mining difficulty adjustment algorithm through a hard fork. We can see that some cryptocurrency systems (e.g., BCH, ETH, and ETC) have often performed hard forks to change their mining difficulty adjustment algorithms [49], [50], [51]. This indicates that cryptocurrency systems can practically update their mining difficulty adjustment algorithms if needed.

In conclusion, if the mining difficulty adjustment algorithm for $coin_{\mathtt{A}}$ is changed to the first type of mining difficulty adjustment algorithms, a lack of loyal miners for $coin_{\mathtt{B}}$ might be reached due to automatic mining.

IX. Discussion

In this section, we first discuss how $coin_{\mathtt{B}}$ can maintain its loyal miners and consider environmental factors that may affect our game analysis results.

A. Maintenance of $coin_{\mathtt{B}}$-loyal miners

As described in Section VIII-B, $coin_{\mathtt{B}}$ cannot prevent the rivalry coin from stealing loyal miners by changing its difficulty adjustment algorithm alone. Surely, the most straightforward way to avoid the risk is to not use the mining hardware compatible with $coin_{\mathtt{A}}$. That is, a proprietary mining algorithm, requiring customized mining hardware which is not compatible with $coin_{\mathtt{A}}$, should be introduced for $coin_{\mathtt{B}}$. However, this solution is not applicable in practice for small and medium-sized mining operators because it is expensive to develop customized mining hardware (e.g., ASICs). In fact, because many altcoins use a mining algorithm that can be implemented in CPU or GPU, automatic mining endangers their mining power, weakening their security.

The second way is to use auxiliary proof-of-work (or merged mining), which makes a miner conduct mining more than two coins at the same time [52]. Therefore, our first assumption in Section IV is not satisfied by merged mining, and our game results would not be applied. This is also regarded as a potential solution to 51% attacks because it significantly increases mining power of altcoins [53]. However, despite of such definite advantages, most projects do not adopt merged mining because of following reasons: It is complex to implement merged mining, and miners should do additional work [53].

The another way is to increase the price of $coin_{\mathtt{B}}$ through price manipulation. However, as far as we know, the problem of maintaining the increased coin price through price manipulation is not well-studied. Moreover, we can consider a way to increase the relative incentive of $coin_{\mathtt{B}}$ mining to $coin_{\mathtt{A}}$ mining, where it can be achieved by increasing the block reward or decreasing the average time of block generation. Even though this method may help prevent the rivalry coin from stealing loyal miners, it would cause other side effects such as inflation or the increase in fork rate [25], [18].

Lastly, $coin_{\mathtt{B}}$ can change its consensus protocol, the PoW mechanism, to another protocol. However, this process would not be supported by existing miners in $coin_{\mathtt{B}}$. For example, Ethereum is planning to switch from a proof-of-work mechanism to a proof-of-stake mechanism for several years. However, note that if the consensus protocol is just changed through a hard fork, the existing miners may leave because they can lose their own merits (e.g., powerful hardware capability) for mining $coin_{\mathtt{B}}$.

B. Environmental factors

In practice, miners' behavior can deviate from our model because of the following environmental factors.

Not all miners are rational. First, miners are not always rational or wise. Even if fickle mining or $coin_{\mathtt{A}}$ mining is more profitable than $coin_{\mathtt{B}}$ mining, some miners may be reluctant to engage in fickle mining or $coin_{\mathtt{A}}$ mining because they may not recognize the profitability in doing so. However, our data analysis confirms that most miners are rational. In addition, if miners use the automatic mining function, they would always follow the most profitable strategy.

Some miners consider the long-term price of coins. Because price prediction is significantly difficult [54], we believe that most miners behave depending on the short-term price of a coin rather than the long-term price. For example, who could have predicted the hash war between ABC and BSV in advance? Therefore, as can be seen from the history of the Bitcoin system, most miners behave depending on short-term profits. To model more realistic and general situations, our model considered both rational miners who are interested in short-term profits and $coin_B$ factions ($\Omega_{\mathtt{stick}}$) which are interested in long-term profits.

Some miners prefer the stable coexistence of coins. Some miners may want the stable coexistence of coins for coin market stability, and they may try to reach the equilibrium representing the coexistence of coins regardless of their profits. If the fraction of such miners is large, a state would move to the equilibrium $(0, \frac{k}{k+1})$ regardless of its zones. Based on historical observations of the Bitcoin system, however, the fraction of these miners seems unlikely to be high in the real-world.

Other selfish mining. In this study, we considered only fickle mining, which is a type of rational mining. However, miners engaging in various form of selfish mining [15], [22], [23], [24] might cause a deviation from our analysis.

X. Conclusion

In this study, we modeled and analyzed the game between two coins for fickle mining, and our results imply that fickle mining can lead to a lack of loyal miners in the less valued coin system. We confirm that this lack of loyal miners can weaken the overall health of coin systems by analyzing real-world history. In addition, our analysis is extended to the analysis of automatic mining, which shows a potentially severe risk of automatic mining. As of Dec. 2018, BCH's loyal miners would leave if more than about 5% of the total mining power in BTC and BCH is involved in automatic mining. Moreover, we explained how one coin can steal the loyal miners from other less valued rivalry coins in the highly competitive coin market by generalizing our game model. We believe that this is one of the serious threats for a cryptocurrency system using a PoW mechanism.

Acknowledgment

We are very grateful to the anonymous reviewers and Andrew Miller, the contact point for major revision of this paper.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[2] "Proof of Work." https://en.bitcoin.it/wiki/Proof_of_work, 2017. [Online; accessed 30-Oct-2017].

[3] "Bitcoin Cash." https://www.bitcoincash.org/, 2018. [Online; accessed 31-May-2018].

[4] Jimmy Song, "Bitcoin Cash: What You Need to Know." https://medium.com/@jimmysong/bitcoin-cash-what-you-need-to-know-c25df28995cf, 2017. [Online; accessed 31-Jun-2018].

[5] Mengerian, "Bringing Stability to Bitcoin Cash Difficulty Adjustments." https://medium.com/@Mengerian/bringing-stability-to-bitcoin-cash-difficulty-adjustments-eae8def0efa4, 2017. [Online; accessed 25-Jul-2018].

[6] "Segregated Witness." https://en.bitcoin.it/wiki/Segregated_Witness, 2018. [Online; accessed 28-Dec-2018].

[7] Jimmy Song, "Bitcoin Cash Difficulty Adjustments." https://medium.com/@jimmysong/bitcoin-cash-difficulty-adjustments-2ec589099a8e, 2018. [Online; accessed 31-Jun-2018].

[8] "ViaBTC." https://pool.viabtc.com/, 2018. [Online; accessed 30-May-2018].

[9] "BTC.com." https://pool.btc.com/pool-stats, 2018. [Online; accessed 30-Jun-2018].

[10] "Bitcoin Cash Hard Fork Plans Updated: New Difficulty Adjustment Algorithm Chosen." , 2017. [Online; accessed 10-Dec-2017].

[11] "Bitcoin Cash's New Hard Fork - How The New Difficulty Algorithm Will Work." https://www.justcryptonews.com/194/bitcoin-cashs-new-hard-fork-how-new-difficulty-algorithm-will-work, 2017. [Online; accessed 10-Dec-2017].

[12] J. A. Kroll, I. C. Davey, and E. W. Felten, "The economics of bitcoin mining, or bitcoin in the presence of adversaries," in *Proceedings of WEIS*, vol. 2013, p. 11, 2013.

[13] B. Johnson, A. Laszka, J. Grossklags, M. Vasek, and T. Moore, "Game-theoretic analysis of DDoS attacks against Bitcoin mining pools," in *International Conference on Financial Cryptography and Data Security*, pp. 72–86, Springer, 2014.

[14] A. Laszka, B. Johnson, and J. Grossklags, "When bitcoin mining pools run dry," in *International Conference on Financial Cryptography and Data Security*, pp. 63–77, Springer, 2015.

[15] I. Eyal and E. G. Sirer, "Majority Is Not Enough: Bitcoin Mining Is Vulnerable," in *International Conference on Financial Cryptography and Data Security*, Springer, 2014.

[16] A. Sapirshtein, Y. Sompolinsky, and A. Zohar, "Optimal selfish mining strategies in bitcoin," in *International Conference on Financial Cryptography and Data Security*, pp. 515–532, Springer, 2016.

[17] K. Nayak, S. Kumar, A. Miller, and E. Shi, "Stubborn mining: Generalizing selfish mining and combining with an eclipse attack," in *Security and Privacy (EuroS&P), 2016 IEEE European Symposium on*, pp. 305–320, IEEE, 2016.

[18] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 3–16, ACM, 2016.

[19] R. Zhang and B. Preneel, "On the necessity of a prescribed block validity consensus: Analyzing bitcoin unlimited mining protocol," in *Proceedings of the 13th International Conference on emerging Networking EXperiments and Technologies*, pp. 108–119, ACM, 2017.
[20] J. Bonneau, "Why buy when you can rent? Bribery attacks on Bitcoin consensus," in *BITCOIN '16: Proceedings of the 3rd Workshop on Bitcoin and Blockchain Research*, February 2016.
[21] Y. Lewenberg, Y. Bachrach, Y. Sompolinsky, A. Zohar, and J. S. Rosenschein, "Bitcoin mining pools: A cooperative game theoretic analysis," in *Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems*, pp. 919–927, International Foundation for Autonomous Agents and Multiagent Systems, 2015.
[22] I. Eyal, "The Miner's Dilemma," in *Symposium on Security and Privacy*, IEEE, 2015.
[23] 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 *Computer Security Foundations Symposium (CSF)*, IEEE, 2015.
[24] Y. Kwon, D. Kim, Y. Son, E. Vasserman, and Y. Kim, "Be Selfish and Avoid Dilemmas: Fork After Withholding (FAW) Attacks on Bitcoin," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pp. 195–209, ACM, 2017.
[25] M. Carlsten, H. Kalodner, S. M. Weinberg, and A. Narayanan, "On the instability of bitcoin without the block reward," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 154–167, ACM, 2016.
[26] I. Tsabary and I. Eyal, "The gap game," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pp. 713–728, ACM, 2018.
[27] J. Bonneau, "Hostile blockchain takeovers (short paper)," in *Bitcoin'18: Proceedings of the 5th Workshop on Bitcoin and Blockchain Research*, 2018.
[28] J. Ma, J. S. Gans, and R. Tourky, "Market structure in bitcoin mining," tech. rep., National Bureau of Economic Research, 2018.
[29] J. Prat and B. Walter, "An equilibrium model of the market for bitcoin mining," tech. rep., CESifo Working Paper, 2018.
[30] "Bitmain." https://bitmain.com/, 2018. [Online; accessed 27-Jul-2018].
[31] Y. Kwon, H. Kim, J. Shin, and Y. Kim, "Bitcoin vs. Bitcoin Cash: Coexistence or Downfall of Bitcoin Cash?," *arXiv preprint arXiv:1902.11064*, 2019.
[32] "Slush." https://slushpool.com/stats/?c=btc, 2018. [Online; accessed 25-Jul-2018].
[33] "CoinWarz." https://www.coinwarz.com/cryptocurrency, 2018. [Online; accessed 30-Jul-2018].
[34] "Daily Bitcoin Cash Profitability Against Bitcoin Summary." https://cash.coin.dance/blocks/profitability, 2018. [Online; accessed 20-Dec-2018].
[35] "BITCOIN CASH ABC VS. BITCOIN CASH SV – EXAMINING THE BITCOIN CASH HASH WAR." https://bitcoinist.com/bitcoin-cash-abc-vs-bitcoin-cash-sv-examining-the-bitcoin-cash-hash-war/, 2018. [Online; accessed 28-Dec-2018].
[36] "Bitcoin.com." https://www.bitcoin.com/, 2018. [Online; accessed 28-Dec-2018].
[37] "AntPool." https://www.antpool.com/home.htm, 2018. [Online; accessed 31-May-2018].
[38] "CoinGeek." https://coingeek.com/, 2018. [Online; accessed 28-Dec-2018].
[39] "Bitcoin Cash (BCH) Mining Pool Mempool Follows Bitcoin SV." https://bitcoinexchangeguide.com/bitcoin-cash-bch-mining-pool-mempool-follows-bitcoin-sv/, 2018. [Online; accessed 30-Dec-2018].
[40] "ViaBTC will support the BCH fork roadmap on bitcoincash.org (PRO ABC!!)." https://www.reddit.com/r/btc/comments/9vr6k3/viabtc_will_support_the_bch_fork_roadmap_on/, 2018. [Online; accessed 30-Dec-2018].
[41] "Jiang Zhuoer: BTC.Top Will Support the Camp Favored by a Majority of Hash Power in the Bitcoin Cash Hash War." https://news.8btc.com/jiang-zhuoer-btc-top-will-support-the-camp-favored-by-a-majority-of-hash-power-in-the-bitcoin-cash-hash-war, 2018. [Online; accessed 30-Dec-2018].
[42] "The Bitcoin Cash Hash War is Over. It Also Ended the BTC/BCH War.." https://coinjournal.net/the-bitcoin-cash-hash-war-is-over-it-also-ended-the-btc-bch-war/, 2018. [Online; accessed 30-Dec-2018].
[43] "Announcement on supporting Bitcoin Cash hard fork." https://pool.viabtc.com/announcement/11/, 2017. [Online; accessed 27-Jul-2018].
[44] "MULTIPOOL." https://www.multipool.us/, 2018. [Online; accessed 27-Jul-2018].
[45] "Digishield v3 problems." https://github.com/zawy12/difficulty-algorithms/issues/7, 2017. [Online; accessed 29-Jul-2018].
[46] "Crypto Compare." https://www.cryptocompare.com/coins/btc/overview/USD, 2018. [Online; accessed 27-Jul-2018].
[47] "Crypto Compare." https://www.cryptocompare.com/coins/bch/overview/USD, 2018. [Online; accessed 27-Jul-2018].
[48] Yujin Kwon, "Automatic mining." https://github.com/dbwls8724/automatic-mining, 2018. [Online; accessed 28-Feb-2019].
[49] Jamie Redman, "Bitcoin Cash Network Completes a Successful Hard Fork." https://news.bitcoin.com/bitcoin-cash-network-completes-a-successful-hard-fork/, 2017. [Online; accessed 09-Jul-2018].
[50] Jeffrey Wilcke, "Ethereum Classic Hard Fork to remove the Difficulty Bomb." https://blog.ethereum.org/2016/02/29/homestead-release/, 2016. [Online; accessed 09-Jul-2018].
[51] Hard fork of Ethereum Classic, "Ethereum Classic Hard Fork to remove the Difficulty Bomb." https://trademarketsnews.com/ethereum-classic-hard-fork-to-remove-the-difficulty-bomb/, 2018. [Online; accessed 09-Jul-2018].
[52] "What is Merged Mining? Can You Mine Two Cryptos at the Same Time?." https://coincentral.com/what-is-merged-mining/, 2018. [Online; accessed 28-Feb-2019].
[53] "What is Merged Mining? — A Potential Solution to 51% Attacks." https://coincentral.com/merged-mining/, 2018. [Online; accessed 28-Feb-2019].
[54] "What will Bitcoin be worth in 2025?." https://www.quora.com/What-will-Bitcoin-be-worth-in-2025?redirected_qid=29574243, 2018. [Online; accessed 31-Dec-2018].