The Miner's Dilemma With Migration: The Control Effect of Solo-Mining

Chuanyun Li
Economics & Technology Research Institute
China National Petroleum Corporation
Beijing, China
lichuanyun@cnpc.com.cn

Florian Spychiger
Blockchain & Distributed Ledger Technologies
UZH Blockchain Center
University of Zurich
Zurich, Switzerland
florian.spychiger@uzh.ch

Claudio J. Tessone
Blockchain & Distributed Ledger Technologies
UZH Blockchain Center
University of Zurich
Zurich, Switzerland
claudio.tessone@uzh.ch

***Abstract*—We consider the "block withholding attack" as introduced by Eyal, where mining pools may infiltrate others to decrease their revenues. However, when two mining pools attack each other and neither controls a strict majority, the so-called miner's dilemma arises. Both pools are worse off than without an attack. Knowing this, pools may make implicit non-attack agreements. Having said this, the miner's dilemma is known to emerge only if no pool controls the majority of the mining power. In this work, we allow for miner migration and show that the miner's dilemma emerges even for pools whose mining power exceeds 50%. We construct a game, where two mining pools attack each other and use simulation analysis methods to analyze the evolution the pools' mining power, infiltration preferences and revenue densities under the influence of different mining pool sizes and miner migration preferences. The results show that underlying game experiences a phase transition fueled by miners' migration preference. Without migration, it is profitable for a large mining pool to attack the other pool. The higher the migration preference of the miners, the more the game transitions into the miner's dilemma and attacking makes both pools worse off. In a second step, we introduce solo-mining into the system. Introducing solo-mining cannot prevent the miner's dilemma, however, it improves the efficiency of the mining process as the infiltration preferences of the mining pools are lowered. Thus, solo-mining has a control effect on the miner's dilemma by keeping the infiltration preference below a certain threshold.**

***Index Terms*—bitcoin, miner's dilemma; block withholding attack; miner migration; solo-mining, evolutionary game theory**

I. Introduction

Bitcoin is still the most popular and most recognized cryptocurrency so far with a market capitalisation of 308 billion US dollar as of November 2020 [1]. Because of its novel decentralized approach, Bitcoin has achieved great success in the digital currency field [2, 3]. Within the underlying blockchain network, nodes create blocks by solving by brute force a computational problem. By this, the network achieves consensus on transactions which is a crucial component of of all blockchain networks [4]. Bitcoin's algorithm is called proof-of-work and it is used in many other platforms [5]. The nodes obtain a certain amount of Bitcoin if they are able to create a valid block [6]. The process of creating blocks is also called *mining*, and the nodes participating in this process are called *miners*. Due to the unstable mining profit of individual miners – as the probability of mining a block is small for a single miner – many miners tend to form mining pools to guarantee stable profit through cooperative mining and profit-sharing [7]. However, in order to maximize their gains, mining pools can let loyal miners infiltrate other mining pools to conduct a pool block withholding attack [7]. The infiltrating miners do not share valid block headers with the infiltrated mining pool leading to a waste of resource for the other honest miners in the pool. This reduces the revenue of the honest miners in the pool. As a result, the Bitcoin mining environment is worsened and it is argued to seriously affect the stability and security of the Bitcoin network [8].

Reference [9] shows that the block withholding attack introduces a miner's dilemma if neither pool controls a strict majority of the mining power: in the Nash equilibrium, both pools attack each other even though they would be better of by not attacking. However, the author does not consider migration. One possible reaction of the honest miners in the attacked mining pool may be to evade the block withholding attack and migrate to another pool to obtain a greater profit. It is important to understand the infiltration behavior of mining pools and the migration behavior of miners within the Bitcoin network in combination. Revealing the evolutionary mechanism of these behaviors helps to improve the mining environment of Bitcoin, and promotes the stable development of the Bitcoin network.

In the recent years, the process of Bitcoin mining has attracted wide attention from the academic community. Some scholars have conducted research on Bitcoin's protocols, the mining pool selection, attack methods, and reward mechanisms [10, 11], [12, 13]. Other have modelled the whole consensus mechanism [14, 15, 16]. Yet others have also explored the impact of transaction fees, of hash rates, of block propagation delays, and of other factors on Bitcoin mining [17, 18, 19]. Early on some people began to study the behavior of mining pools and miners in Bitcoin from a game-theoretic perspective [19, 20, 21]. Some scholars use evolutionary game theory to study the security of Bitcoin mining by constructing a

978-1-6654-3924-4/21/$31.00 ©2021 IEEE

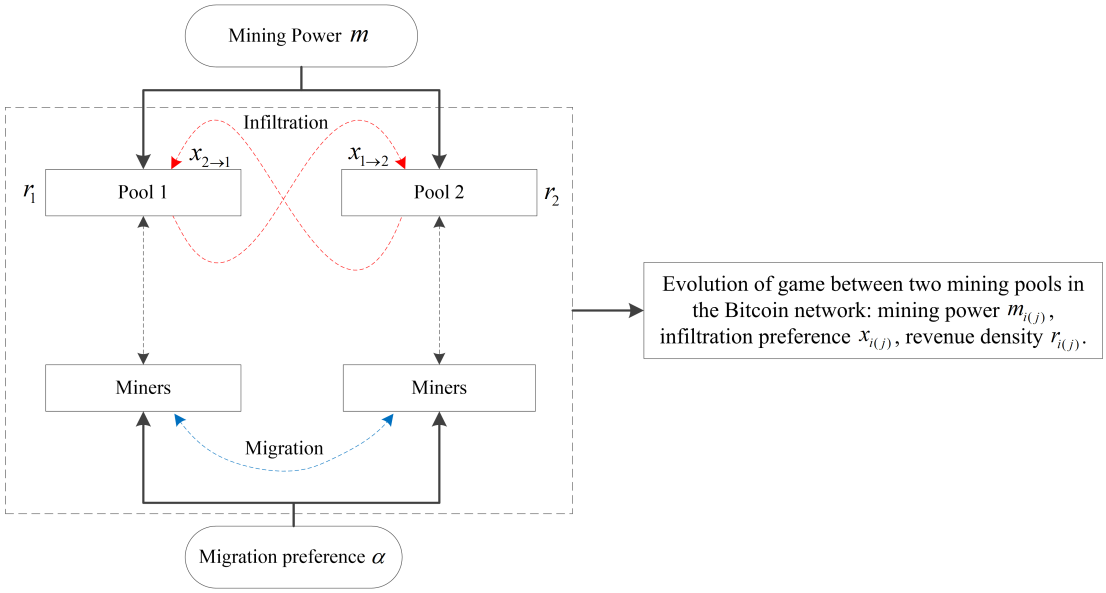


Fig. 1: Evolutionary analysis framework (extended version of [9])

game model for the process of Bitcoin mining [22, 23, 24]. Others have also from the perspective of Nash equilibrium, put forward zero-determinant strategy and deep gradient learning strategies to optimize the process of mining strategy selection to solve the mining dilemma [25, 26]. Within this context, the mining process in Bitcoin under mutual attack between mining pools has been studied. For example, [27] constructs an iterative game model of miner mining under the mutual attack of two mining pools, and proposes a zero-determinant strategy for solving the dilemma of miners. Reference [28] built a game model of mutual attacks between mining pools and found that an increase of the attack costs and the basic migration rate of miners can reduce the possibility of mutual attacks between mining pools. Reference [29] built a game model of mutual attacks under different mining pool sizes, studied the impact of mining pool size on attack motivation, and found that larger mining pools have greater attack motivation. Reference [30] established a game model between mining pools based on the PoW consensus algorithm, and found that the mining pool can increase its infiltration rate and average income by increasing the mining pool power and the betrayal rate of miners. Reference [31] built a game model of mutual attacks between mining pools and study the impact of different block withholding (BWH) attack intensity on miners' income. It is found that only when the BWH attack intensity is lower than a certain threshold, it can lead to an improvement of miners' income in the mining pool, so as to attract more miners to join the mining pool. In [32] the relationship between miner migration and mining pool rewards is studied, and it is found that it is almost impossible to distribute rewards in a stable way, and some miners always migrate between mining pools. Reference [33] empirically analyzed the migration behavior of miners among 15 mining pools in the history of Bitcoin and found that miners are a typical economic entity seeking to maximize profits. With respect to the migration process, [34] considers the relationship between the random migration level of miners and the average earnings of miners, and constructs a concurrent mean return game model (CMPG) to analyze the motivation to deviate from honest behavior. [35] found that changes in the profit of neighboring mining pools will lead to changes in the attractiveness of the pool and may lead to random migration of miners between the pools.

The previous game-theoretic research on mutual attacks of mining pools has been very fruitful. However, the above work still has the following two main deficiencies: (1) Most scholars have only analyzed the impact of either the mining pool or the miners' behavior on average earnings, ignoring the interaction between mining pools and miners. (2) The withholding attack has only been explored without migrating miners with the exception of [36]. This work is based on this model and we extend the analysis by additionally considering individual miners - so called solo-miners.

In view of this, we consider the game model of [9] on mutual attacks of mining pools and extend it to account for migration of miners (see Figure 1). This allows us to explore the interaction between mining pools and miners. We construct a game model based on evolutionary game theory, where mining pools select the optimal infiltration rate x – that can also be zero – and miners can migrate. The miners are profit-driven and therefore, they self-select whether they want to migrate by comparing past revenues of the pools. If they migrate, they will migrate a share α of their mining power. Since the migration rule is probabilistic and involves non-linear relationships, we cannot solve the model analytically. Therefore, we use a simulation to analyze the evolution of the mining pool's mining power m, infiltration preferences x and revenue densities r (i.e. average earnings) under the influence of different initial mining pool powers m and miner migration

preferences α. We show that the miner's dilemma introduced by [9] for pools with mining power of less than 50% emerges also for pools controlling a strict majority of the mining power once migration is taken into account. Furthermore, a phase transition takes place once migration is introduced. The miner's dilemma does not emerge without migration and the stronger the migration preference become, the more the game changes into an iterative prisoner's dilemma that is played by the mining pools. In a second step, we introduce the option of solo-mining in the model. Introducing solo-mining does not eliminate this iterative prisoner's dilemma, however, the presence (or threat) of solo miners enhances the mining efficiency as mining pools opt for lower infiltration rates. Reference [9] suggests that the block withholding attack does rarely occur in the Bitcoin network since the pools know that they would end up in this sub-optimal situation. Knowing this fact, pools may have reached implicit agreements to not attack each other. We provide further indication that this holds true even if one pool dominates the mining power – given that miners migrate. According to the argument of [9], this non-attack situation is unstable and eventually, one pool will decide to attack as this can be done anonymously. As a consequence, miners will form smaller private pools which leads to more fine-grained mining power distribution and a potentially better situation for the Bitcoin mining environment (in terms of reduced concentrations). Whether this mechanism really takes place in practice is questionable, as the atomization of mining pools is not observed. We argue that even though the miner's dilemma emerges also in a network with highly concentrated mining power distribution, it does not induce the aforementioned mechanisms and positive impacts on the Bitcoin mining environment.

Our contributions are therefore:

1) Extending the game model of [9] with migration.
2) Modeling the interaction between mining pools and miners with respect to the block withholding attack.
3) Showing that the miner's dilemma emerges also for pools controlling a strict majority of the mining power.
4) Showing the control effect of solo-mining on the infiltration preferences of the mining pools.

The remainder of this paper is organized as follows. The foundations of the evolutionary analysis framework of the two mining pool game in the Bitcoin network is presented in section II. Then, the game model of the two mining pools game in the Bitcoin network is introduced in section III. Subsequently, the simulation results of two mining pools under mutual attack are illustrated in section IV. Finally, Section V concludes.

II. Model Foundations

With the increasing value of Bitcoin, mining has become a fast-growing industry [37]. But in the mining process, only the most advanced mining equipment produces profit, otherwise, the cost exceeds expected profit. If we consider a node with a small computing power with respect to the whole network, the probability it mines a block is low. Thus, most of the miners usually organize themselves into mining pools to obtain a more stable profit [9]. Mining pools are ad hoc groups of many miners who share computational resources to mine blocks together. When a miner in the mining pool succeeds in mining, the revenue is distributed among the mining pool members according to their mining capacity. Due to the combined computational power, mining pools can find blocks at a higher rate, which makes the mining pool obtain more frequent revenue, thereby ensuring that the miners can obtain a more stable profit.

In the process of Bitcoin mining, some mining pools adopted pool block withholding attacks to maximize their own profits [7]. The attacking miners register with the infiltrated mining pool and start mining, but the attacking miners only send a part of their proof of work. If the attacking miners find a solution that constitutes a complete proof of work, they discard it, so that the total revenue of the attacked mining pool is reduced. This decreases the revenue of the attacking miners and, therefore, this attack can only be used for sabotage.

If the attacked mining pool is in such an environment for a long time, its members, under the dual influence of their own profits and the profits of neighboring mining pool miners, might choose a migration strategy, which ultimately makes the attacked mining pool paralyzed and it may collapse because it cannot maintain the normal operation of a mining pool. On the long-term, this will lead to the gradual deterioration of the mining environment and the emergence of oligopoly mining pools. However, the attacked pool may choose to defend itself by infiltrating the other pool as well.

Based on this, we build an evolutionary analysis framework for the two mining pools game in the Bitcoin network. We embed the pools' attack behavior and miner's migration behavior into the game model of the two mining pools, thereby extending the model of [9]. The total mining power in the network is m, where the mining pool power in mining pool 1 is $m_1 > 0$, the mining pool power in mining pool 2 is $m_2 > 0$ and we have $m = m_1 + m_2$. Mining pool i controls the infiltration of mining pool j to $x_{i \to j}$. We denote the migration preference of the pools by α. When a miner migrates, a miner will take a share α of its mining capacity away from the mining pool and transfer it to the other mining pool. The higher α, the stronger is the migration. As shown in Figure 1, we can explore the evolution of the pool's mining power, infiltration preference and revenue density by varying the pool sizes and the miner migration preferences.

III. Game Model

A. Basic Assumptions of the Model

To study the effects of migration on the miners' rewards, we keep the model as parsimonious as possible. In particular, we consider only two large mining pools as this suffices to understand the basic mechanics of the block withholding attack with migration. Furthermore, having only two pools allows us to study fully a setting where one pool has a majority of the mining power. Introducing additional pools implied also a substantial mathematical overhead and further

assumptions on the migration dynamics.Therefore, based on the characteristics of the game between the mining pools and practical considerations, we make the following assumptions

i.) In the Bitcoin network, there are only two large mining pools and all miners depend on the mining pool to obtain revenue.
ii.) All miners have the same individual mining capacity (they are identical).
iii.) Pools and miners maximize profits.
iv.) Pools can select their infiltration preference.
v.) Miners in the mining pool are bounded rational agents, and can only choose between two strategies: migration and non-migration. When a miner migrates, a miner will take a share α of its mining capacity away from the mining pool and transfer it to the other mining pool.
vi.) Miners use a unified strategy update rule of memory length 1, that is, the miner's strategy selection depends on the result of the previous round.

Since all miners are identical, the total number of miners does not matter in the model. It is only the ratio of mining power that they allocate to a certain pool that is relevant, in particular since a miner can participate in both pools by dividing their minging power. It is important to acknowledge that a two pool setup implies a hidden assumption that we would like to make explicit: In a two pool setup, one pool has always the majority of the mining power and could in principle earn all the rewards [38]. However, we argue that a rational mining pool would not do such an extreme attack because it destroys the idea of a decentralized currency leading to a negative price impact (and therefore to lower returns). Therefore, the mining pools consider less dystopian attacks such as a the Block-Withholding attack.

B. Construction of The Game Model

We draw on [9] to construct the game model presented by Equations (1) - (8). During the first round $(t = 1)$ game, the total mining power is m, with $m = m_1 + m_2$. The effective mining power of mining pool 1 is $m_1 - x_{1\to2}$. Likewise, the effective mining power of mining pool 2 is $m_2 - x_{2\to1}$. The total effective mining power in the Bitcoin network is therefore $m-x_{1\to2}-x_{2\to1}$. The direct revenue share R_1 of mining pool 1 and R_2 of mining pool 2 are their effective mining rates. That is the mining power excluding the infiltration, divided by the total effective mining power:

$$R_1 = \frac{m_1 - x_{1\to2}}{m - x_{1\to2} - x_{2\to1}} \tag{1}$$

$$R_2 = \frac{m_2 - x_{2\to1}}{m - x_{1\to2} - x_{2\to1}} \tag{2}$$

The sum of the direct revenue shares always equals 1, i.e. this reflects the distribution of the fixed block reward between the mining pools. However, during each round of the game, there are two sources of revenue for the mining pool. One part is the direct mining revenue brought by the faithful miners' honest mining, and the other part is the indirect revenue of the infiltration miners attacking the neighboring mining pool, that is, the total revenue of the attacked mining pool multiplied by its infiltration rate. At the same time, the mining pool distributes the total revenue to its registered miners. Therefore, the revenue of each miner in mining pool 1 (denoted by r_1) and mining pool 2, that is, the revenue density is:

$$r_1 = \frac{R_1 + x_{1\to2}r_2}{m_1 + x_{2\to1}} \tag{3}$$

$$r_2 = \frac{R_2 + x_{2\to1}r_1}{m_2 + x_{1\to2}} \tag{4}$$

Therefore, the revenue density measures the total revenue of honest mining and of attacking the neighboring pool, while the latter revenue is not a monetary reward, but rather the indirect gain of reducing the nominal mining power of the other pool. The revenue density therefore is dependent on the strategies of the other miners.While the direct profits R_i always add up to 1 – the reward is fixed in the system –, the revenue densities are not a zero-sum game, since the revenue densities expresses the relative advantages with respect to the mining pools' revenues.

Solving for r_1 and r_2, we express the revenue density as a function of $x_{1\to2}$ and $x_{2\to1}$. As the calculation is straightforward, we omit the proof.

$$r_1(x_{1\to2}, x_{2\to1}) = \frac{m_2R_1 + x_{1\to2}(R_1 + R_2)}{m_1m_2 + m_1x_{1\to2} + m_2x_{2\to1}} \tag{5}$$

$$r_2(x_{2\to1}, x_{1\to2}) = \frac{m_1R_2 + x_{2\to1}(R_1 + R_2)}{m_1m_2 + m_1x_{1\to2} + m_2x_{2\to1}} \tag{6}$$

C. The Optimal Infiltration Rate

Each mining pool selects the infiltration rate in order to obtain the maximum profit r for its miners. The pool can also decide not to attack the other pool by setting the infiltration rate to zero. Therefore, in each round t, the mining pools calculate the best infiltration rate $x_{1\to2}$ and $x_{2\to1}$ as follows:

$$x_{1\to2}(t) \leftarrow \arg\max_{x'} r_1(x', x_{2\to1}(t-1)) \tag{7}$$

$$x_{2\to1}(t) \leftarrow \arg\max_{x'} r_2(x', x_{1\to2}(t-1)) \tag{8}$$

As shown by [9], for any pool size m_1 and m_2 ($0 < m_1$, $0 < m_2$, $m_1+m_2 \leq m$), a unique solution exists. In particular, for our model with $m_1 + m_2 = m$, the solution exists and is unique.

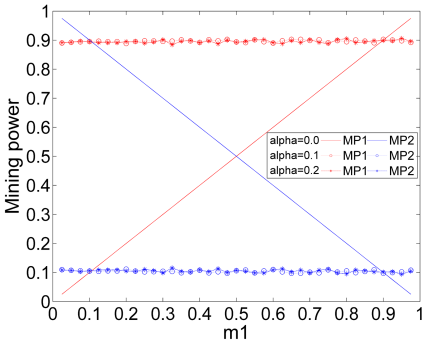
D. The Migration Rule

If the honest miners in pool i migrate a share α in time t to pool j, then the mining power of pool j increases accordingly in the next period. Therefore, the higher α, the more mining power is migrated and the stronger the migration. We model the migration dynamics as:

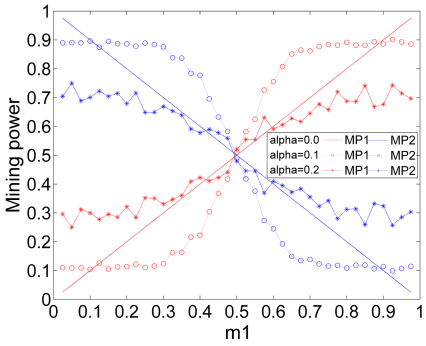
$$m_j(t+1) = m_j(t) + \alpha \times [m_i(t) - x_{i\to j}(t)] \tag{9}$$

The honest miners compare their profits in pool i to the profits of the miners in the neighboring pool j. However, since

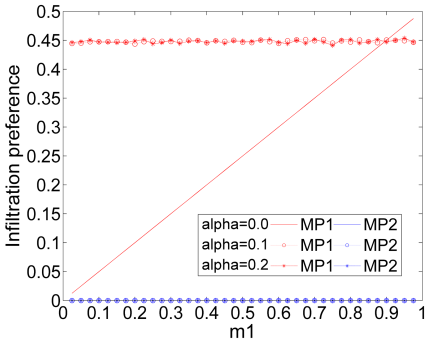
This article has been accepted for publication in IEEE Transactions on Network and Service Management. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TNSM.2022.3232183



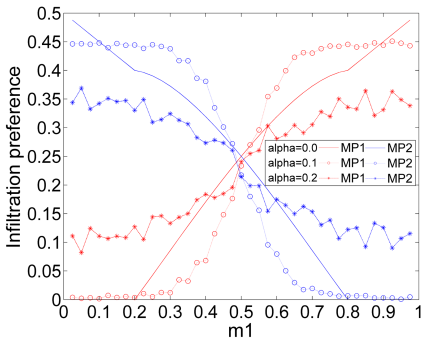
(a) **Only pool 1 attacks:** The changes of the mining power with respect to the initial mining power m_1 and three different migration preferences α of the miners.



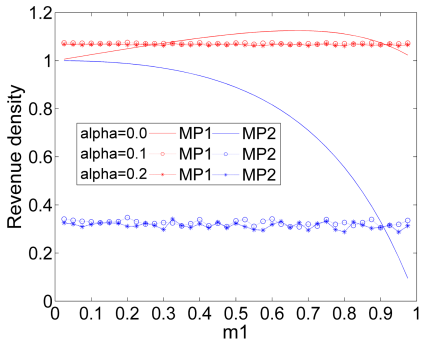
(b) **Both pools attack:** The changes of the mining power with respect to the initial mining power m_1 and three different migration preferences α of the miners.



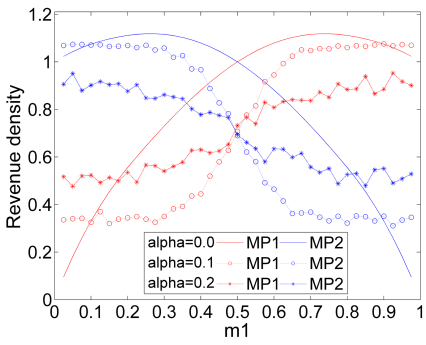
(c) **Only pool 1 attacks:** The changes of the infiltration preference with respect to the initial mining power m_1 and three different migration preferences α of the miners.



(d) **Both pools attack:** The changes of the infiltration preference with respect to the initial mining power m_1 and three different migration preferences α of the miners.



(e) **Only pool 1 attacks:** The changes of the revenue density with respect to the initial mining power m_1 and three different migration preferences α of the miners.



(f) **Both pools attack:** The changes of the revenue density with respect to the initial mining power m_1 and three different migration preferences α of the miners.

Fig. 2: The mining power, the infiltration preference and the revenue density of the two pools for three different α and varying m.

the miners are bounded rational agents, they are not perfect decision-makers. Therefore, if the profit in the neighbouring pool is larger, they will only migrate a share α of their mining power with a certain probability $W_{i\to j}$ in the next round of the game. If they were fully rational agents, they would set this probability always equal to one if the profit of the other pool is larger. The probability $W_{i\to j}$ is usually calculated by the Fermi function [39] under the standard assumption of bounded rational agents:

$$W_{i\to j} = \left[1 + \exp\left(\frac{r_i(t-1) - r_j(t-1)}{K}\right)\right]^{-1} \tag{10}$$

where K represents the noise intensity, That is, the decision-making mistakes and bounded rationality characteristics of miners. When $K \to 0$, it means that miners will not be disturbed by external factors and carry out rational strategy choice. When K diverges, it means that miners are irrational due to external interference and can only update their strategies randomly. The Fermi-rule allows for a comparison of the different strategies, i.e., the miners select the best strategy given the strategies of all other miners. However, one cannot study the benefit of one strategy in isolation as the payoffs depend on the actions of the other miners.

IV. Simulation Analysis

A. Simulation Setting

According to the introduced evolutionary model, we solve the complex model with an simulation. The simulation steps under the mutual attack of the two mining pools are set as follows:

1) Initialize the parameters of the simulation.
2) In time step t of the game, the miners compare their previous profits with the miners of the neighboring mining pool and decide whether to migrate a share α.
3) The mining pools decide on their infiltration rate $x(t)$ based on the previous profits.
4) At the end of time step t, calculate the new profits.
5) At the beginning of $t+1$, repeat Step 2 and Step 3 until reaching the the final time step T, and the simulation is stopped.

At the start of the simulation $(t = 0)$, we set the total mining power $m = 1$ and we select a noise factor $K = 0.5$

as it is often done in literature. We conduct the simulation for different values of m_1, m_2, and α. We run the simulation for all size combinations of m_1 and m_2, where $m_1 = 1 - m_2$. Further, we analyse three different scenarios: 1) no migration ($\alpha = 0$), 2) moderate migration ($\alpha = 0.1$), and 3) strong migration ($\alpha = 0.2$). Having said this, $\alpha > 0$ does not mean that miners need to migrate, but they can migrate if it is beneficial for them according to the Fermi rule (equation 10). We use Matlab2020a to conduct the simulation analysis. We simulate the game for $T = 500$ time steps. To ensure the accuracy of the results, we average the results over 100 runs for each parameter setting.

B. The Mining Power

In the model, the mining power m_2 can be expressed as $1 - m_1$. As a consequence, one mining pool always controls a strict majority of the mining power. In Subfigure 5a, only pool 1 attacks, i.e. $x_{2\to1} = 0$. In this case, it does not matter whether the miner has a moderate ($\alpha = 0.1$) or a strong ($\alpha = 0.2$) preference for migration. We will see this invariance in all of the subsequent analysis for the one-pool-attacks scenario. Interestingly here, even an initially small pool is able to gain a strict majority of the mining power in the long run. This is not true for the both-pools-attack scenario shown in Subfigure 5b. In all three migration scenarios, the pool initially controlling the majority of the mining power still controls the majority at the end. With $\alpha = 0$, we recover the model of [9] as no migration takes place. In this case, there is no dynamic evolution of the mining power over time and the mining powers remain constant. However, in presence of moderate migration ($\alpha = 0.1$), the behavior changes. There are two regimes: in the first, when $m_1 \in (0.0, 0.3) \cup (0.7, 1.0)$, the mining powers gravitate towards a high (90%) resp. low (10%) level irrespective of the initial mining power. At a certain critical point ($m_1 \approx 0.3$), the second regime begins and the mining power increases (resp. decreases) rapidly. Furthermore, the larger pool tend to profit from moderate migration as they are able to gain mining power over time. Only very large pools with a mining power $m > 0.9$ lose some miners to the smaller one. If migration preference is higher ($\alpha = 0.2$), however, the largest pool is worse off than without migration. Similarly, we observe again two regimes: In the first, miners migrate to the other pool leading to lower discrepancy between the mining powers; in the second, miners' migration cancels out and the initial mining powers remain more or less constant. Therefore, small pools tend to gain mining power, whereas large pools tend to lose miners.

C. The Optimal Infiltration Rate

As [9] already noted, there is a certain threshold for the size of a mining pool that is needed such that an infiltration attack is considered worthwhile. In the one-pool-attacks scenario (Subfigure 2c), the pool that has the possibility to attack will always choose to do so (as $m \approx 0.9$, see Subfigure 5a). As before, the magnitude of the miners' migration preference does not matter. As shown in Subfigure 2d, with no migration, the pools do not attack if $m < 0.2$. However, with migration, there are at least some small attacks for moderate migration and larger attacks for strong migration. Since the size of the mining pools is not static anymore and changes during the simulation, the infiltration preferences change respectively. In the case of moderate migration, the logic of [9] is recovered. Since in the first regime ($m_1 \in (0.0, 0.3) \cup (0.7, 1.0)$), the mining power of the smaller pool stabilizes around 0.1, the infiltration preference is the same as with no migration at $m_1 = 0.1$ resp. $m_1 = 0.9$, i.e. represented by the intersection of the lines with no migration and moderate migration in Figure 2d. Once the migration preference of the miners becomes stronger, the infiltration once again assimilates and both pools will always attack. Initially small mining pools consider an attack worthwhile as well, since they are able to reach a considerable size. The whole dynamics is an iterative adaption process between the mining pools and the miners: at time t, the miners decide to migrate and the mining pool sets the optimal infiltration rate. Their decisions are based on the decisions of each other (as well as on the other mining pool and its miners) at time $t - 1$.

D. The Emergence of the Prisoner's Dilemma

If none of the pools attacks, the revenue density is for both pools equal to one if the total mining power is $m = 1$. To see this, consider equation (3) and (4) with $x_{1\to2} = x_{2\to1} = 0$ and $m = 1$. Reference [9] has showed that a prisoner's dilemma exists when neither mining pool controls the majority of the mining power. Concretely, he shows that when two pools with $m_1 < 0.5$ and $m_2 < 0.5$ attack each other, both obtain a revenue density $r < 1$, but attacking is still their best strategy. However, this is only valid under the condition that none of the pools controls a strict majority of the mining power. In our model, one of the pools always (except in the edge case of $m_1 = 0.5$) controls a strict majority. In this scenario, [9] shows that the pool controlling the majority can always improve its revenue compared to the no-pool-attacks scenario. To see this, consider Figure 2 in the no migration case ($\alpha = 0$). Subfigure 5e shows the one-pool-attacks scenario if pool 1 attacks, however, due to symmetry, the results hold true for pool 2 as well. The attacking pool can earn a revenue larger than its fair share irrespective of its initial size m, whereas the attacked pool earns a revenue lower than one. If both pools attack (Subfigure 5f), the larger mining pool ($m > 0.5$) always earns a revenue bigger than one in the no migration case and the smaller pools earns less than one. Therefore, attacking is a dominant strategy for the larger pool as its revenue is larger than one. This can be modelled as a game and is shown in table I, where we denote the revenue of the smaller pool with r_s and the revenue of the larger pool with r_l. For the smaller pool, it depends on the initial mining power m_s whether to attack. However, without migration attacking is clearly a dominant strategy for the larger pool.

If there is strong migration ($\alpha = 0.2$), the game has changed. In the one-pool-attacks scenario, the revenue of the attacked pool is below 0.4 no matter what is its initial size m.

Small Pool \ Large Pool	no attack	attack
no attack	$1, 1$	$r_s < 1, r_l > 1$
attack	$r_s > 1, r_l < 1$	$r_s < 1, r_l > 1$

TABLE I: Dominant strategy game without migration ($\alpha = 0$).

Furthermore, in the two-pools-attack scenario, the revenues for the larger pools are below one and the revenues for smaller pools larger than 0.4. The exact values depend on the initial sizes m, but it is clear that the revenue densities are below one. As a result, we recover the miner's dilemma of [9]. Table II shows the payoff matrix for the miners. Here, it becomes clear that with strong migration, we end up with the both-pools-attack Nash equilibrium. Even though both pools would be better off by not attacking each other, they both attack, hence, it is a classic prisoner's dilemma.

Small Pool \ Large Pool	no attack	attack
no attack	$1, 1$	$r_s \ll 1, r_l > 1$
attack	$r_s > 1, r_l \ll 1$	$r_s < 1, r_l < 1$

TABLE II: Miner's dilemma for strong migration ($\alpha = 0.2$).

Interestingly, taking migration into account leads once again to the prisoner's dilemma also when one pool controls a strict majority. However, the effect depends on the migration intensity. The case of moderate migration ($\alpha = 0.1$) is mixture between the dominant-strategy game ($\alpha = 0$) and the prisoner's dilemma ($\alpha = 0.2$) depending on the exact value of m_1. Therefore, the game goes through a phase transition depending on the migration parameter α.

E. The Strength of Migration

In Figure 3, we show the effect of varying the miner's migration preference α. For large differences in the initial mining power ($m_1 = 0.05$), the larger pool loses mining power with migration for all value of α. However, the larger mining pool is able to retain about 90% of the mining power even for moderate migration ($\alpha = 0.1$). After this, the differences in mining power decline rapidly and at a value of $\alpha \approx 0.35$ it vanishes. With such strong migration, the initial large difference in mining power does not play a role anymore as migration leads to an assimilation of both pools. This observation holds true for other initial configurations if the migration is that strong ($\alpha \geq 0.35$). For lower values of migration preference, however, the pool that has a larger initial mining power is able to gain mining power over time.

The optimal infiltration preference in Sub-figure 3b chosen by the mining also varies with the parameter α. If the migration preference of the miners becomes stronger ($\alpha > 0.1$), the small pool starts to attack. The optimal infiltration rate x depends also on the eventual size of the mining pool. Therefore, the infiltration rate assimilates and stabilizes at a value of 0.25.

With respect to the the revenue density, we can observe that the emergence of the miner's dilemma depends on α, but also on the initial mining power m of the pools. If the initial mining powers of the pools are very similar, the miner's dilemma emerges even for small value of α. In other words, the game transitions already with little migration into the miner's dilemma. When one pool controls a large majority of the initial mining power (e.g. 90%), then it requires strong migration such that the miner's dilemma emerges.

F. Accounting for Solo-Mining

To make the model more realistic, we relax assumption i.*(In the Bitcoin network, there are only two large mining pools and all miners depend on the mining pool to obtain revenue.)* as follows: We allow solo-mining, meaning that the miners may leave (or join) mining pools 1 and 2 if they want and start to mine solo. They can also decide to join a pool again in case solo-mining is not worthwile. So, all migration paths are possible (solo-mining to pool / pool to pool / pool to solo-mining). If they decide to mine solo, they cannot infiltrate mining pools and *vice versa* cannot be infiltrated by others. It is a priori not clear whether solo-mining is more or less beneficial than mining in a pool. However, solo-mining is feasible at all times since miners in the network can always join and leave pools (they have the equipment anyways). The payoffs of solo-mining depend again on the actions of the other miners.

The combined mining power of all solo-miners is denoted by m_{sm}. Therefore, we have that $m = m_1 + m_2 + m_{sm}$. As a result, the direct revenue share R_{sm} of the solo-miners is given by

$$R_{sm} = \frac{m_{sm}}{m - x_{1\to 2} - x_{2\to 1}} \tag{11}$$

The direct revenue is the mining power of the solo miners divided by the total effective mining power and therefore, depends on the strategies of the other miners. There is no infiltration rate for the solo miners since they cannot infiltrate other. Similarly, the revenue density of the solo miners does only consist of their direct revenue divided by their total mining power:

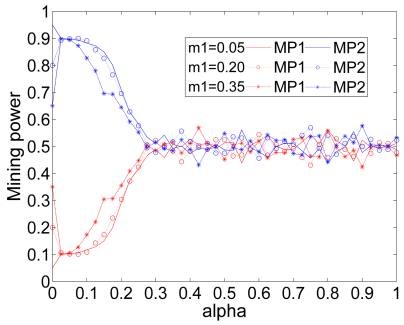
$$r_{sm} = \frac{R_{sm}}{m_{sm}} = \frac{1}{m - x_{1\to 2} - x_{2\to 1}} \tag{12}$$

Furthermore, we assume the same migration preference α for the solo miners as for the pool miners. The pools again try to select the optimal infiltration rate as in equations 7 and 8. For the migration between the pools and also when pool miners become solo miners, we will use the same dynamics as in equation 9. If solo miners migrate to mining pools, the migration dynamics is simply given by

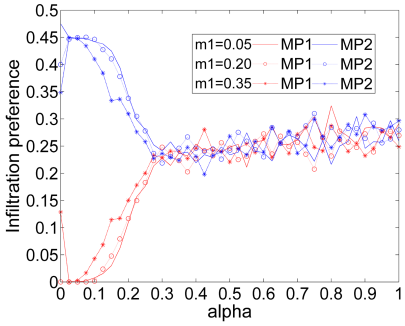
$$m_i(t+1) = m_i(t) + \alpha \times m_{sm}(t) \tag{13}$$

Again, miners compare their profits with either a pool or solo mining and migrate a share α of their mining power with probability W_i in the next round of the game. To keep the model simple, we assume the following two-step approach:

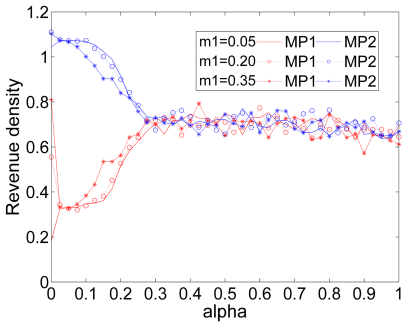
This article has been accepted for publication in IEEE Transactions on Network and Service Management. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TNSM.2022.3232183



(a) **Both pools attacks:** The changes of the mining power with respect to the migration preference α and three different initial mining powers m_1 of the miners.



(b) **Both pools attack:** The changes of the infiltration preference with respect to the migration preference α and three different initial mining powers m_1 of the miners.



(c) **Both pools attack:** The changes of the revenue density with respect to the migration preference α and three different initial mining powers m_1 of the miners.

Fig. 3: The average mining power, infiltration preference, and revenue density for three different m and varying α.

1) Randomly decide on the counterpart to compare the profit to, i.e. with a probability of 0.5 for each party.
2) Apply the Fermi update rule [39] to construct the migration probability $W_{i\to j}$:

$$W_{i\to j} = \left[1 + \exp\left(\frac{r_i(t-1) - r_j(t-1)}{K}\right)\right]^{-1} \quad (14)$$

We used the same simulation settings as described in subsection IV-A, however, we set initial share of the solo miners $m_{sm} = 0.01$ for all simulations. This makes the comparison possible between the setting without solo-mining possible. With such an (almost) negligible initial mining power of the solo miners, we can still explore the effects of migration on large mining pools ($m_i > 50\%$). As it will show, the initial mining power of the solo miners does not influence the outcome. Even more, with solo mining, the mining power, the infiltration preference, and the revenue density becomes independent of the initial mining power distribution.

Figures 4 shows the adapted framework. While the mining pools still have the option for infiltration, the solo miners do not take part in the infiltration game. However, they are part of the migration dynamics since pool miners can become solo miners and *vice versa*. We then again measure the mining power m_i, the infiltration preference $x_{i\to j}$, and the revenue density r_i.

In Figure 5, we show the results with solo miners included. We again differentiate among no migration ($\alpha = 0$), moderate migration ($\alpha = 0.1$), and strong migration ($\alpha = 0.2$). However, by looking at Figure 5, it becomes immediately clear that the strength of migration does not influence the results. Nevertheless, migration within the system has an influence. Therefore, we differentiate only between no migration $\alpha = 0$) and migration ($\alpha > 0$) for the further analysis.

Solo-mining seems a valuable option for the miners once they can migrate. In the equilibrium, a mixture between pool-mining and solo-mining emerges. This means that solo-mining is feasible and also beneficial for some of the miners. However, this is only true as long as a substantial share (about 60%) of the other miners join a pool. If too many miners mined solo, mining in a pool become again more attractive. Therefore, in the equilibrium, both is needed.

Interestingly, the conceptual results with respect to the miner's dilemma remain the same with the introduction of solo miners. If there is no migration, the revenue densities are as in Table I and attacking is a dominant strategy for the larger pool. Again, the optimal strategy of the smaller pool depends on the initial mining power m_s. Likewise, with migration, the payoffs for the small and large pools are the same as in the case without solo mining (Table II). Consequently, the miner's dilemma emerges and we end up with the both-pools-attack Nash equilibrium.

Even though the outcome of the game remains unchanged by introducing solo-mining, it has some interesting consequences for the system. As for the mining power, the game calibrates to a healthy state where neither pool has a majority of the mining power (Figure 5a and 5b). The option of solo-mining in an attack-prone environment leads to a more decentralized setup and a more efficient mining power allocation.

A similar effect takes place with respect to the infiltration preference. Figure 5c and 5d show the infiltration preference for different initial mining pool sizes m_1, while the initial $m_{sm} = 0.01$. Without migration, the optimal infiltration preference for the pools are capped by about 0.36, even for larger pools ($m_i > 0.9$) who could allocate much higher proportions to attacking the smaller pool – and without solo-mining, they also do so (Figure 2. With migration, the attacking pool allocates only very little mining power to infiltration attacks (Figure 5c). If both pools attack, they allocate exactly the same amount of mining power to infiltration attacks. Again, compared to the case without solo-mining, the infiltration preferences in the system are much lower (Figure 2). Therefore, the presence of solo-mining results into lower infiltration preferences. The reason for this can be found in the solo miners' profit and revenue density equations 11 and 12. The larger the infiltration preferences of the pools, the larger is the profit resp. the revenue density of solo mining. As a

This article has been accepted for publication in IEEE Transactions on Network and Service Management. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TNSM.2022.3232183

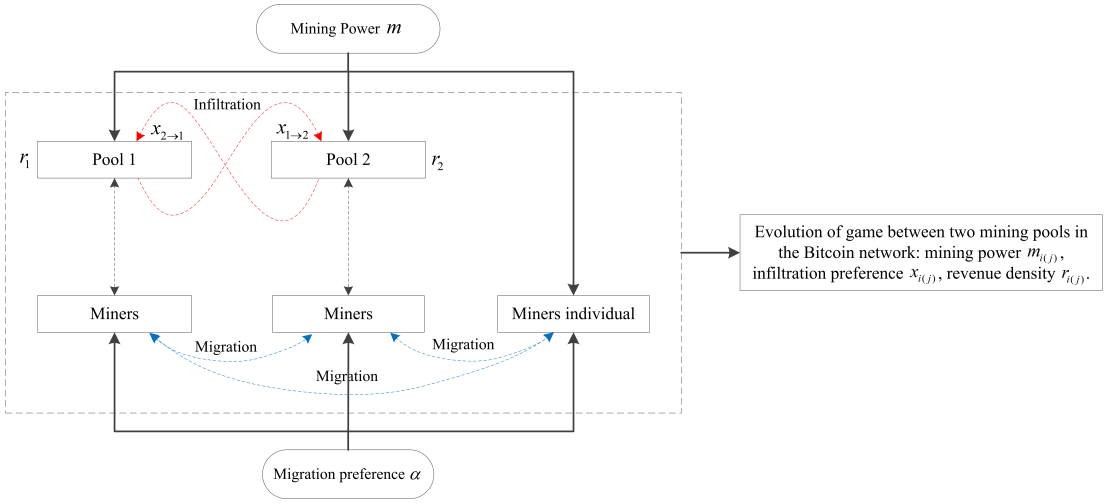
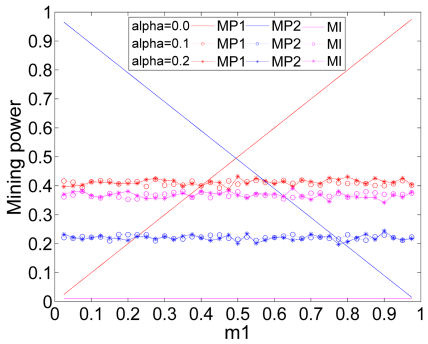
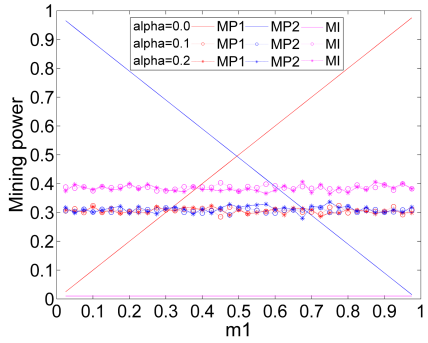


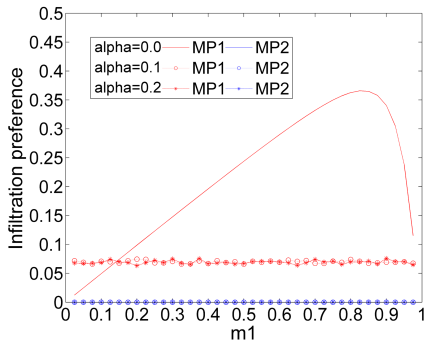
Fig. 4: Evolutionary analysis framework (include miners individual)



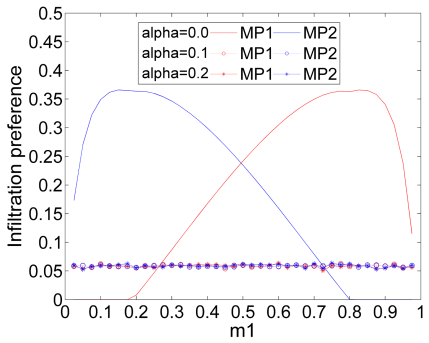
(a) **Only pool 1 attacks:** The changes of the mining power with respect to the initial mining power m_1 and three different migration preferences α of the miners.



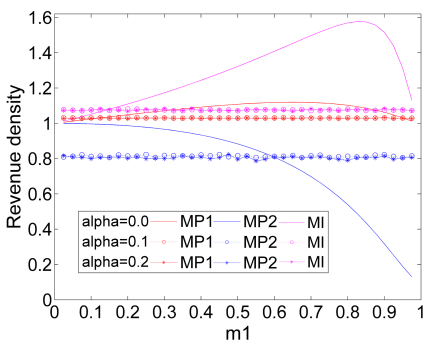
(b) **Both pools attack:** The changes of the mining power with respect to the initial mining power m_1 and three different migration preferences α of the miners.



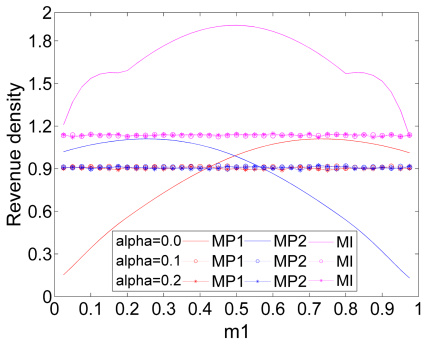
(c) **Only pool 1 attacks:** The changes of the infiltration preference with respect to the initial mining power m_1 and three different migration preferences α of the miners.



(d) **Both pools attack:** The changes of the infiltration preference with respect to the initial mining power m_1 and three different migration preferences α of the miners.



(e) **Only pool 1 attacks:** The changes of the revenue density with respect to the initial mining power m_1 and three different migration preferences α of the miners.



(f) **Both pools attack:** The changes of the revenue density with respect to the initial mining power m_1 and three different migration preferences α of the miners.

Fig. 5: The mining power, the infiltration preference and the revenue density of the two pools for three different α and varying m with individual miners.

consequence, the infiltration preferences cannot be too high as otherwise the miners would start solo-mining and leave the pools. As a consequence, the pools cannot select a too high infiltration preference. The presence of solo-mining does not prevent the miner's dilemma, but it increases the efficiency of mining as the mining pools opt for lower infiltration rates and the total effective mining power $m - x_{1\to2} - x_{2\to1}$ in the system increases.

In Figure 6, we show that varying the miner's migration preference α does not have an effect. Even for large differences in the initial mining power ($m_1 = 0.05$), both pools converge to about 30% of the mining power, while the solo-miners secure 40% of the mining power. This remains the same for almost all migration preferences α. Only for very large migration preferences ($\alpha > 0.7$), the solo-miners retain even a bit more of the mining power. However, overall the mining power, the infiltration preference and the revenue density become independent of the migration preferences (with the exception of very high values). The additional option of solo-mining allows the miners to more efficiently allocate their mining power, since they have now a broader set of alternatives.

V. Conclusion

Considering the migration process of miners in a proof of work system, we extend the model of Eyal to study the mutual infiltration attack between two mining pools if one pool controls a strict majority of the mining power. We show that the miner's dilemma emerges for all initial pool sizes if the migration is strong enough. After a certain migration preference of the miners has been surpassed, even extremely large pools suffer from the miner's dilemma. With solo-mining, even small to moderate migration is sufficient to trigger the miner's dilemma for all pool sizes. This result may help to explain why the block withholding attack has been rarely observed in Bitcoin. Even though a few mining pools are jointly controlling the majority of the mining power in Bitcoin, block withholding attacks do not occur. Our results show that with migration, also large pools must fear the miner's dilemma and it is therefore probable that implicit non-attack agreements exist. However if the sole mechanism would be the miner's dilemma, ultimately one pool would attack as this situation is unstable. Consequently, the other pool would also attack leading to lower revenues for both pools and miners would leave the mining pools to form smaller (private) pools leading to an improved mining environment. This effect is also indicated by considering solo-mining, which could also be considered as small private pools that do not participate in the infiltration game. In the presence of such solo-miners, the large mining pools will confine their infiltration rates to low values. Furthermore, the system ends up in a state where neither of the pool controls a strict a majority of the mining power. Therefore, the possibility of solo-mining increases not only the decentralization in the system, but also safeguards the system against too much infiltration activities. Therefore, designers of blockchain protocols should strive for a decentralized mining setup as this increases the options for miners. This again increases the incentives for mining pools to act honestly as otherwise miners would migrate to more profitable alternatives than being forced to participate in a detrimental miner's dilemma game.

Our work here suffers from certain limitations: We applied a relatively straightforward migration model which might not adequately captures the migration dynamics. Further, we neglected pool fees in our analysis. We also made some simplifying assumptions such that all miners have the same mining power. In addition, miners are profit-maximizing, however, they might also be variance-minimizing. Lastly, we only looked at a two pool setting. For future work, we plan to extend on our work as follows: We want to include several pools as well as multiple distinct miners that also minimize the variance of the return streams. We also want to explore other migration dynamics to check the robustness of our results. Additionally, we want to conduct an in-depth evaluation of our theoretical results with data from the real Bitcoin network. Finally, we will explore why the block withholding attack does not occur in practice, since there are other mechanisms than the miner's dilemma at play as well. All in all, we hope to contribute to a better understanding of the mining environment in proof of work blockchain-based systems.

Acknowledgment

CL acknowledges the support from the Graduate School of Harbin Engineering University that enabled a research stay at UZH.

References

[1] "blockchain.com." https://www.blockchain.com/prices. Accessed: 2020-11-16.

[2] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of trust: A decentralized blockchain-based authentication system for iot," *Computers & Security*, vol. 78, pp. 126–142, 2018.

[3] M. C. Kus Khalilov and A. Levi, "A survey on anonymity and privacy in bitcoin-like digital cash systems," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2543–2585, 2018.

[4] P. Tasca and C. Tessone, "A taxonomy of blockchain technologies: Principles of identification and classification," *Ledger*, vol. 4, no. 0, 2019.

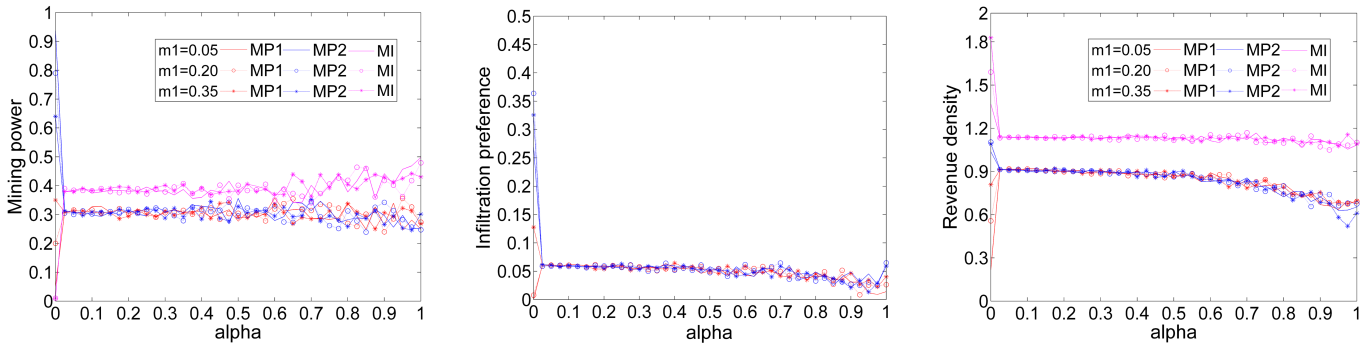
[5] F. Spychiger, P. Tasca, and C. J. Tessone, "Unveiling the importance and evolution of design components through the "tree of blockchain"," *Frontiers in Blockchain*, vol. 3, 2021.

[6] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2009.

[7] M. Rosenfeld, "Analysis of bitcoin pooled mining reward systems," *arXiv preprint arXiv*, vol. 1112, 12 2011.

[8] N. T. Courtois and L. Bahack, "On subversive miner strategies and block withholding attack in bitcoin digital currency," *arXiv preprint arXiv*, vol. 1402, 1 2014.

[9] I. Eyal, "The miner's dilemma," in *2015 IEEE Symposium on Security and Privacy*, pp. 89–103, 2015.



(a) **Both pools attack:** The changes of the mining power with respect to the migration preference α and three different initial mining powers m_1 of the miners.

(b) **Both pools attack:** The changes of the infiltration preference with respect to the migration preference α and three different initial mining powers m_1 of the miners.

(c) **Both pools attack:** The changes of the revenue density with respect to the migration preference α and three different initial mining powers m_1 of the miners.

Fig. 6: The average mining power, infiltration preference, and revenue density of the two pools and the solo-miners for three different m and varying α.

[10] X. Dong, F. Wu, A. Faree, D. Guo, Y. long Shen, and J. feng Ma, "Selfholding: A combined attack model using selfish mining with block withholding attack," *Computers & Security*, vol. 87, p. 101584, 08 2019.

[11] R. Qin, Y. Yuan, and F. Wang, "Research on the selection strategies of blockchain mining pools," *IEEE Transactions on Computational Social Systems*, vol. 5, no. 3, pp. 748–757, 2018.

[12] R. Recabarren and B. Carbunar, "Hardening stratum, the bitcoin pool mining protocol," *Proceedings on Privacy Enhancing Technologies*, vol. 2017, pp. 57–74, 3 2017.

[13] O. Schrijvers, J. Bonneau, D. Boneh, and T. Roughgarden, "Incentive compatibility of bitcoin mining pool reward functions," in *Financial Cryptography and Data Security - 20th International Conference, FC 2016, Revised Selected Papers* (B. Preneel and J. Grossklags, eds.), Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), pp. 477–498, Springer Verlag, 2017. 20th International Conference on Financial Cryptography and Data Security, FC 2016 ; Conference date: 22-02-2016 Through 26-02-2016.

[14] C. J. Tessone, P. Tasca, and F. Iannelli, "Stochastic modelling of blockchain consensus," 2021.

[15] E. Fadda, J. He, C. Tessone, and P. Barucca, "Consensus formation on heterogeneous networks," 2021.

[16] C. Schwarz-Schilling, S.-N. Li, and C. J. Tessone, "Agent-based modelling of strategic behavior in pow protocols," in *2021 Third International Conference on Blockchain Computing and Applications (BCCA)*, pp. 111–118, IEEE, 2021.

[17] D. Easley, M. O'Hara, and S. Basu, "From mining to markets: The evolution of bitcoin transaction fees," *Journal of Financial Economics*, vol. 134, no. 1, pp. 91–109, 2019.

[18] J. Göbel, H. Keeler, A. Krzesinski, and P. Taylor, "Bitcoin blockchain dynamics: The selfish-mine strategy in the presence of propagation delay," *Performance Evaluation*, vol. 104, pp. 23 – 41, 2016.

[19] Z. Liu, N. C. Luong, W. Wang, D. Niyato, P. Wang, Y.-C. Liang, and D. I. Kim, "A survey on applications of game theory in blockchain," *arXiv preprint arXiv*, vol. 1902, 2 2019.

[20] A. Kiayias, E. Koutsoupias, M. Kyropoulou, and Y. Tselekounis, "Blockchain mining games," in *Proceedings of the 2016 ACM Conference on Economics and Computation*, EC '16, (New York, NY, USA), p. 365–382, Association for Computing Machinery, 6 2016.

[21] S.-N. Li, Z. Yang, and C. J. Tessone, "Proof-of-work cryptocurrency mining: a statistical approach to fairness," in *2020 IEEE/CIC International Conference on Communications in China (ICCC Workshops)*, pp. 156–161, IEEE, 2020.

[22] D. Kraft, "Game-theoretic randomness for blockchain games," *arXiv preprint arXiv*, vol. 1901, 1 2019.

[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 *2015 IEEE 28th Computer Security Foundations Symposium (CSF)*, pp. 397–411, IEEE Computer Society, 2015.

[24] E. K. Wang, C.-M. Chen, S. M. Yiu, M. M. Hassan, M. Alrubaian, and G. Fortino, "Incentive evolutionary game model for opportunistic social networks," *Future Generation Computer Systems*, vol. 102, pp. 14 – 29, 2020.

[25] C. B. Tang, Z. Yang, Z. L. Zheng, and Z. Y. Cheng, "Analysis and optimization of game dilemma in pow consensus algorithm," *Acta Automatica Sinica*, vol. 43, no. 9, pp. 1520–1531, 2017.

[26] T. T. Wang, S. Y. Yu, and B. M. Xu, "Research on proof of work mining dilemma based on policy gradient algorithm," *computer application*, vol. 039, no. 005,

pp. 1336–1342, 2019.

[27] Z. Yang, Y. Miao, Z. Y. Chen, C. B. Tang, and X. Chen, "Zero-determinant strategy for the algorithm optimize of blockchain pow consensus," in *2017 36th Chinese Control Conference (CCC)*, pp. 1441–1446, 2017.

[28] A. Laszka, B. Johnson, and J. Grossklags, "When bitcoin mining pools run dry: A game-theoretic analysis of the long-term impact of attacks between mining pools," pp. 63–77, 2015.

[29] B. Johnson, A. Laszka, J. Grossklags, M. Vasek, and T. Moore, "Game-theoretic analysis of ddos attacks against big and small mining pools," in *1st Workshop on Bitcoin Research, in association with FC 2014 (BITCOIN)*, vol. 8438, 08 2014.

[30] W. B. Li, M. W. Cao, Y. Wang, C. B. Tang, and F. L. Lin, "Mining pool game model and nash equilibrium analysis for pow-based blockchain networks," *IEEE Access*, vol. 8, pp. 101049–101060, 2020.

[31] F. Kentaro, Z. Yuanyu, S. Masahiro, and K. Shoji, "Mining pool selection under block withholding attack," *Applied Sciences*, vol. 11, p. 1617, 2 2021.

[32] 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*, AAMAS '15, (Richland, SC), p. 919–927, International Foundation for Autonomous Agents and Multiagent Systems, 2015.

[33] N. Tovanich, N. Soulié, N. Heulot, and P. Isenberg, "An empirical analysis of pool hopping behavior in the bitcoin blockchain," in *2021 IEEE International Conference on Blockchain and Cryptocurrency*, 5 2021.

[34] K. Chatterjee, A. K. Goharshady, R. Ibsen-Jensen, and Y. Velner, "Ergodic mean-payoff games for the analysis of attacks in crypto-currencies," *arXiv preprint arXiv*, vol. 1806, 6 2018.

[35] A. T. Haghighat] and M. Shajari, "Block withholding game among bitcoin mining pools," *Future Generation Computer Systems*, vol. 97, pp. 482 – 491, 2019.

[36] C. Li, F. Spychiger, and C. J. Tessone, "The miner's dilemma with migration," in *2021 3rd Conference on Blockchain Research Applications for Innovative Networks and Services (BRAINS)*, pp. 97–104, 2021.

[37] N. Popper, "Into the bitcoin mines," *The New York Times*, vol. 163, no. 56358, pp. 1–4, 2013.

[38] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," *Commun. ACM*, vol. 61, p. 95–102, jun 2018.

[39] G. Szabó and C. Tőke, "Evolutionary prisoner's dilemma game on a square lattice," *Phys. Rev. E*, vol. 58, pp. 69–73, Jul 1998.