

Selfish Mining in Proof-of-Work Blockchain with Multiple Miners: An Empirical Evaluation*

Tin Leelavimolsilp^{1**}, Viet Nguyen², Sebastian Stein¹, and Long Tran-Thanh¹

¹ University of Southampton, Southampton, SO17 1BJ, UK
{tin.leelavimolsilp,s.stein,l.tran-thanh}@soton.ac.uk

² Imperial College London, London, SW7 2AZ, UK
viet.nguyen17@imperial.ac.uk

Abstract. Proof-of-Work blockchain, despite its numerous benefits, is still not an entirely secure technology due to the existence of Selfish Mining (SM) strategies that can disrupt the system and its mining economy. While the effect of SM has been studied mostly in a two-miners scenario, it has not been investigated in a more practical context where there are multiple malicious miners individually performing SM. To fill this gap, we carry out an empirical study that separately accounts for different numbers of SM miners (who always perform SM) and strategic miners (who choose either SM or Nakamoto's mining protocol depending on which maximises their individual mining reward). Our result shows that SM is generally more effective as the number of SM miners increases, however its effectiveness does not vary in the presence of a large number of strategic miners. Under specific mining power distributions, we also demonstrate that multiple miners can perform SM and simultaneously gain higher mining rewards than they should. Surprisingly, we also show that the more strategic miners there are, the more robust the systems become. Since blockchain miners should naturally be seen as self-interested strategic miners, our findings encourage blockchain system developers and engineers to attract as many miners as possible to prevent SM and similar behaviour.

Keywords: Selfish mining · Proof-of-Work blockchain · Agent-based model · Empirical multiplayer game

1 Introduction

With the aim to decrease reliance on financial institutions, blockchain was designed and used to securely approve and record transactions among Internet

* This is the author's accepted version of the work. The final authenticated version is maintained by Springer Nature Switzerland AG and is available online at https://doi.org/10.1007/978-3-030-33792-6_14.

** Corresponding author

users [11]. A number of blockchain characteristics such as its security, transparency, and decentralised authority have drawn many researchers and developers to apply blockchain to a wide range of application areas, such as personal data management [1,16], Internet of Things [5], and decentralised platform as a service [14].

The success of blockchain is based on two elements: an application of a cryptographic puzzle, namely Proof-of-Work (PoW), and an economic incentive for miners, who are the underlying workforce of the system. The mining process is briefly described as follows. First, a miner composes a block which mainly consists of locally verified transactions. The block also refers to the latest block of the miner’s locally stored blockchain as its parent block. The miner then performs a brute force search for a number that results in a hash value of the block lower than the globally set target. When such a number (which is a “Proof of Work” that the miner did) is found, the block together with the number is broadcasted. Subsequently, a recipient of the block verifies the block’s transactions and the block’s hash value. Once approved, the block is then appended to the recipient’s locally stored blockchain. Later, the miner claims their mining reward (which is the aforementioned incentive) by referring to the block in their spending transaction. As such, every miner is fairly rewarded in proportion to a number of blocks that they managed to create or an amount of hash rate that they expended.¹

One of the most fundamental and significant attacks against blockchain systems is *forking*, which is difficult in practice and widely known as the 51% attack. Since the mining protocol instructs everyone to trust the longest chain², a malicious miner simply needs to produce a blockchain longer than the current one. Once succeeded, part of the current blockchain will be replaced by the malicious miner’s blocks. Consequently, all transactions and the mining reward of the replaced blocks have been nullified, and the malicious miner earns all mining reward from their blocks; thus resulting in a disproportionate reward distribution. However, forking is not easy since it requires at least a half of the total hash rate in the system [11]. As such, it resulted in a public belief that blockchain systems are strongly secure as long as no miner possesses more than 50% of the total hash rate.

Eyal and Sirer later demonstrated that forking is still possible with lower hash rates using their *Selfish Mining* (SM) strategy [6]. Essentially, SM hides and privately mines their own blocks in contrast to publicly forking the blockchain. Such hiding allows the malicious miner to gain an advantage by removing the chance of the successive blocks being mined by the others. In addition, SM

¹ To be precise, there are two types of mining reward: namely, block reward and transaction fee [2]. While there will be no block reward per block in the future, miners will still be incentivised by the transaction fee to do their mining.

² In practice, a chain that is the most computationally expensive or has the highest difficulty sum is always chosen [4]. If every block has the same computational difficulty (as assumed in this work), the actual verification reduces to selecting the longest blockchain.

gradually discloses their private blocks to keep the advantage as much as possible to themselves. Most importantly, it requires only $\frac{1}{3}$ of the total hash rate to fork the blockchain and earn a higher mining reward than they should. Such a low hash rate is significantly lower than $\frac{1}{2}$ of the total hash rate for publicly forking, and therefore greatly threatens the security of blockchain systems. With a larger hash rate, SM is even more effective and can fork the blockchain more frequently. In the worst scenario, the mining economy and the system could collapse due to the disrupted distribution of the economic incentive.

Moreover, SM can be difficult to detect in practice. While the rate of orphaned blocks (i.e. blocks that were not part of the longest chain) is a main indicator of SM activity [8], it can point out a network instability or a high network delay that causes broadcasted blocks to arrive late or be lost. As such, the practicality of the detection method based on the orphaned block rate is not certain.

Despite the threats posed by SM, there are not sufficient investigations in a more practical context: that is, a case where SM being used individually and simultaneously by multiple miners. In particular, most research so far focused on a system with one malicious miner who performs SM and has another who follows Nakamoto’s mining protocol [6,7,9,12,13,15]. In practice, multiple miners can perform SM at the same time. Whether SM is even more effective in such situation is not clearly known.

For this reason, we carry out an investigation on SM in the context of multiple miners. Particularly, we seek to know (a) the effectiveness of SM in such a context, (b) the minimum hash rate that SM requires to earn mining reward more than it should, and (c) the minimum hash rate that non-malicious miners require to prevent SM. We also consider strategic miners who choose either SM or Nakamoto’s mining protocol depending on which gives a higher mining reward. We believe that such miners better represent the actual miners since earning mining reward is the main purpose of their mining activity and they would prefer a higher reward.

The rest of this paper is structured as follows. First, a literature review of existing studies on SM is presented. We then describe two models of PoW blockchain systems (where one considers strategic miners and the another does not) and some concepts that are necessary for our work. Subsequently, our empirical results for each model are described and discussed. We finally conclude this paper with our findings and interesting questions that remain to be solved.

2 Related Work

After Eyal and Sirer’s work, there has been further research on improving SM. To exemplify this, the optimised (two-miners) SM strategy was proposed and its effectiveness was slightly improved [7,13]. A combination of SM with other attacks was also designed to increase the effectiveness of the attack [12]. In general, such improvements further reduce the amount of required hash rate to successfully employ SM.

A number of studies also shed more light on SM under different contexts. For example, Göbel et al., who further explored the effect of network delay on the SM strategy, demonstrated that SM will be more successful if every miner in the SM pool³ helps propagate the hidden block [8]. Kiayias et al. also showed that, under the game-theoretical setting, every miner will follow Nakamoto’s mining protocol if no one has a hash rate greater than 30.8% of the total hash rate [9].

On the contrary, a number of improvements of Nakamoto’s mining protocol have been suggested, but they are difficult to implement in practice [6,15]. In particular, the improvements which raises the hash rate required for SM to be effective needs a precise coordination among miners to adopt them at the same time.

Despite the significant body of work on SM, the idea of multiple miners individually and simultaneously employing SM has not been fully explored in the existing literature. In particular, most works so far studied SM or similar strategies in a setting with one malicious miner and one non-malicious miner [6,7,9,12,13,15]. To our knowledge, there is a small-scale study which was recently conducted in parallel [10]. Compared to their work, our findings are more robust due to a large number of malicious miners in the system and a fair treatment of the underlying network in our experiment. Our work also offers a game-theoretical analysis which is a natural extension when malicious miners are considered self-interested agents that act strategically to maximise their mining rewards.

3 Models of the PoW Blockchain Mining

In this section, we formally define two models of Proof-of-Work (PoW) blockchain mining where the difference between them lies in the miner’s capability of choosing a mining strategy. To clearly observe the effect of varying number of miners upon SM, assumptions are made as follows:

1. A fully connected network of miners without any communication delay;
2. An equal amount of mining reward per block to the creator of every block in the blockchain; and
3. The same computational difficulty (the target hash value) for every block in the blockchain.

We consider two mining strategies: *Honest Mining (HM)* and *Selfish Mining (SM)*⁴. The first is Nakamoto’s mining protocol where a miner always mines and publishes a new block from the last block of the longest blockchain. On the other hand, the latter is a strategy that hides its recently created block to privately mine from it and then strategically publishes its hidden blocks to overwrite the others’ blocks in the currently longest chain [6]. That is, whenever

³ A pool is a group of miners whose mining processes are coordinated such that they receive their individual mining rewards in a smaller chunk more frequently comparing to solo mining [3].

SM receives a new block created by the others, SM also publishes its block with the expectation that it reaches the rest of the network more quickly than the received block. If SM's block reaches first, the another block will be ignored. In addition, SM publishes all hidden blocks to completely overwrite the other chain whenever the SM's branch is longer by one. At any time, SM always mines the deepest block, and it abandons its chain entirely whenever another chain is longer.

Subsequently there are three types of miners: Honest miner, Selfish miner, and Strategic miner. By definition, Honest miner and Selfish miner perform HM and SM respectively; henceforth HM and SM will also be used to denote them. In contrast, *Strategic miner (StrM)* is a miner that uses either the HM or SM strategy depending on which maximises its mining reward. Note that StrM will be referred to only in the second model where we consider miners are capable of choosing their strategies.

3.1 Fixed Strategy Mining Model

Here, we describe the first model of the PoW blockchain mining process where every miner employs a fixed mining strategy. Formally, a Markov model of the fixed strategy mining $\mathcal{M} = (I, C, P, S, \mathbb{P}(\cdot), \mathbb{U}(\cdot))$ is as follows:

- $I = \{1, 2, \dots, N\}$ denotes a set of all miners individually represented by a positive integer.
- $C = (c_i | c_i \in \{\text{HM}, \text{SM}\}, i \in I)$ is a list of miner's mining strategies where the i -th element is a mining strategy used by the i -th miner in I .
- $P = (p_i | p_i \in [0, 1], \sum_{i \in I} p_i = 1, i \in I)$ is a tuple of miner's *mining powers* where the i -th element is the i -th miner's proportion of the total hash rate. That is, P is a power allocation or power distribution of miners in the system.
- S is a set of all states in this Markov model where each element $s \in S$ is a state of the blockchain. Note that the initial state $s_0 \in S$ is the blockchain with only one block that is not owned by any miner in I .
- $\mathbb{P}(\cdot)$ is a state transition function where its probability mass is $\mathbb{P}(s_{t+1} | s_t) = p_i$, and the next state s_{t+1} is the current state s_t that includes the new block created by miner i . In other words, a transition from state s_t to state s_{t+1} represents a discovery of a new block with respect to miner's mining powers.
- $\mathbb{U}(\cdot)$ is a utility function that gives the converged value of the proportion of a miner's blocks in the longest blockchain. Given a sufficiently long time t and a state $s_t \in S$ that has only one longest chain of blocks, the i -th miner's *mining reward* $\mathbb{U}(s_t, i)$ can be computed as follows:

$$\mathbb{U}(s_t, i) = \frac{b_i}{\sum_{i \in I} b_i} \quad (1)$$

⁴ We do not use the optimised (two-miners) SM [7,13] since it might not be optimal in our context of multiple miners. The method of obtaining an optimal strategy in this context is also not yet known and lies outside the scope of this work.

where b_i is the total number of i -th miner's blocks in the longest chain starting from the initial block in s_0 . Since this is a stationary Markov model, there always exists the convergence time t where $\forall t_1, t_2 \in [t, \infty) : |\mathbb{U}(s_{t_1}, i) - \mathbb{U}(s_{t_2}, i)| \leq \alpha$ and α is a negligible positive number.

3.2 Dynamic Strategy Mining Model

In contrast to the previous model, the model here considers the malicious miner's capability of choosing a mining strategy that maximises their individual mining reward. With a game analysis of this model, we account for a change of the SM miner's strategy when they deem it is better off to use HM under some power allocations.

In particular, we extended the previous model such that every SM miner becomes a StrM miner who chooses their mining strategy given information of other miners' available strategies and all possible mining rewards that the StrM miner will receive. In particular, an empirical normal-form game of the PoW mining is denoted by $\mathcal{G} = (I, C', P, \mathbb{A}(\cdot), \mathbb{U}'(\cdot))$ where I and P are the same as before and the rest are described as follows:

- $C' = (c'_i | c'_i \in \{\text{HM}, \text{StrM}\}, i \in I)$ is a list of miner's types where the i -th element indicates whether an i -th miner is a HM miner or a StrM miner.
- $\mathbb{A}(\cdot)$ is a function that maps a type of miner to a set of strategies. Given an i -th miner's type $c'_i \in C'$, the function $\mathbb{A}(\cdot)$ is formally described as follows.

$$\mathbb{A}(c'_i) = \begin{cases} \{\text{HM}, \text{SM}\} & \text{if } c'_i = \text{StrM} \\ \{\text{HM}\} & \text{otherwise} \end{cases}$$

Consequently, a strategy profile is denoted as $A = (a_i | a_i \in \mathbb{A}(c_i), c'_i \in C, i \in I)$ or $A = (a_i, a_{-i})$ where a_i is the i -th miner's strategy and a_{-i} collectively denotes the rest.

- $\mathbb{U}' : I \times A^N \mapsto [0, 1]$ is a payoff function that computes a miner's mining reward. Given a strategy profile A , the value of $\mathbb{U}'(i, A)$ is simply retrieved from the utility function \mathbb{U} of the previously described model \mathcal{M} where its strategy list C corresponds to $A \in \mathcal{G}$ and other elements of the model are the same.

4 Power Threshold, Safety Level and Equilibrium

As mentioned in Section 1, we are interested in the minimum mining power that enables SM/StrM miners to earn an unfairly large amount of mining reward and the minimum total sum of mining power of all HM miners that can prevent such an unfair outcome.

In more detail, an unfairly large mining reward in our models is one that exceeds the miner's mining power. Originally, a system of all HM miners, in the long run, will allocate a mining reward equal to a miner's mining power (since

everyone mines from the latest block and the expected proportion of miner's blocks is the miner's power.) However, a miner with sufficiently high mining power can use SM and gain a mining reward that is higher than their mining power. Such an unfairly large reward is demonstrated in the next section of this paper.

In our discussion, we then look for a *power threshold* which is the least mining power that lets SM/StrM earn its unfairly large mining reward regardless of how much mining power the others possess. Consequently, a SM/StrM miner whose mining power reaches the power threshold will always earn a mining reward that is more than they should.

Definition 1 Given $\hat{P}, (p)$ the set of all possible power allocations where a SM/StrM miner has mining power p , and $\mathbb{U}_{p,P}$, the mining reward of the SM/StrM miner with mining power p in a power allocation P , a **power threshold** β is one that satisfies the following condition:

$$\beta = \min \{ p \mid \forall P \in \hat{P}(p) : \mathbb{U}_{p,P} > p ; \quad \forall q \in [p, 1], \forall P' \in \hat{P}(q) : \mathbb{U}_{q,P'} > q \}$$

In other words, for every SM/StrM's mining power that yields mining reward larger than the power regardless of the others' power, a power threshold is the least power of SM/StrM that also yields such a reward for every SM/StrM's power beyond the threshold.

Similarly, we also search for a *safety level*, which is the least mining power of a collective of all HM miners that prevents all SM/StrM miners from earning their unfairly large mining reward. Once the safety level is reached, no SM/StrM miner will be able to gain a mining reward that is higher than their mining power.

Definition 2 Given I' , the set of all SM/StrM miners, and \mathbb{U}_{i,p_i} , the mining reward of the i -th miner with mining power p_i , a **safety level** γ is one that satisfies the condition below:

$$\gamma = \min \{ p_{HM} \mid \forall P \in \hat{P}(p_{HM}), \forall i \in I'(P) : \mathbb{U}_{i,P} \leq p_{i,P} ; \\ \forall q_{HM} \in [p_{HM}, 1], \forall P' \in \hat{P}(q_{HM}), \forall i' \in I'(P') : \mathbb{U}_{i',P'} \leq p_{i',P'} \}$$

where $\hat{P}(p)$ is the same as in Definition 1 and p_{HM} is a mining power sum of all HM miners.

That is, for every mining power of an HM collective that results in all SM/StrM's mining rewards being no greater than their power regardless of how much power all SM/StrM individually have, a safety level is the collective's least power that also yields such SM/StrM's rewards for every HM collective's power beyond the safety level.

In the dynamic strategy mining model (Section 3.2), we will retrieve an outcome of the game prior to an analysis of the safety level and the power threshold. In particular, we use the concept of pure-strategy ϵ -equilibrium (ϵ -PE) to derive the choice of miners' strategies that maximises their mining reward. The concept is also useful to disregard small fluctuations in the payoff value; such a fluctuation is caused by a stochastic nature of the PoW blockchain mining process and consequently could lead us to misinterpret the result.

Definition 3 A pure-strategy ϵ -equilibrium (ϵ -PE) where $\epsilon > 0$ is a strategy profile $A^* = (a_i^*, a_{-i})$ that satisfies the following condition:

$$\forall i \in I, \forall a_i \in \mathbb{A}(c_i') : \mathbb{U}'(i, A^*) \geq \mathbb{U}'(i, (a_i, a_{-i})) - \epsilon$$

In other words, for each and every miner, there are no other mining strategies that allow them to gain a higher utility than the strategy in the pure-strategy ϵ -equilibrium by ϵ , given that the others' strategies are fixed.

Finally, an extra assumption where HM is more preferable to SM will be incorporated in the ϵ -PE analysis of the result. In the next section, we show the existence of multiple equilibria due to a negligible difference between HM's and SM's mining reward in the same power allocation. Since there is neither an incentive nor a proper reason for StrM to use SM instead of HM in such cases, we disregard such equilibria with SM by the *HM-preference assumption*, which is defined as follows:

Definition 4 Given a pair of ϵ -equilibria $A^* = (a_i^*, a_{-i})$ and $A^{**} = (a_i^{**}, a_{-i})$ where $a_i^* \neq a_i^{**}$ (one i -th miner's choice is HM and the another is SM) under the same instance of model \mathcal{G} , an HM-preferable ϵ -equilibrium is the equilibrium where the i -th miner's choice is HM.

5 Empirical Results and Discussion

To address our research question, we carry out discrete event simulations of the models such that different numbers of SM/StrM miners and different power allocations are accounted.⁵ Each simulation setting is also repeatedly simulated 100 times to compute an average of the converged utility value. In a rare case of non-convergence, we use the value at the 200,000th timestep, which is analogous to 3-4 years in the Bitcoin system and well approximates the system behaviour compared to the results of others [6,13].

Table 1: Simulation parameters

	Parameter	Value
	α (Equation 1)	0.0001
	ϵ (Definition 3)	0.0001
Power step	for 1,2,3 SM/StrM cases	0.01
	for 4 SM/StrM case	0.02
	for 5,6,7 SM/StrM cases	0.04
	for 8,9 SM/StrM cases	0.05

⁵ Note that modelling the underlying network is out of scope of this work. Consequently multiple broadcast messages that occurred in single timestep were processed in a uniformly random manner.

Due to the extremely large number of required simulations, we carry out simulations only for the base parameters and perform permutation to cover all necessary results. To exemplify this, we swap the miner’s utility values of the model \mathcal{M}_1 with $C_1 = (\text{HM}, \text{SM})$ and $P_1 = (0.4, 0.6)$ and use it as a result of the model \mathcal{M}_2 where $C_2 = (\text{SM}, \text{HM})$ and $P_2 = (0.6, 0.4)$. We also treated a collective of HM miners as a single HM miner since their individual earning is unnecessary in this work and an overall outcome of their individual mining is the same as mining done by one HM with their combined mining powers in our models.

5.1 Fixed Strategy Mining

In general, the mining powers of SM and HM that yield an unfairly large mining reward decreases with the number of SM miners in the system. As shown in Figure 1(a), the mean of SM’s mining reward among different power allocations exponentially grows in an increase of SM’s mining power until its convergence at one. However, the range of SM’s mining power during the exponential growth gradually decreases with the number of SM miners. A similar trend in the HM’s mining reward with respect to the HM’s mining power is also observed and shown in Figure 1(b).

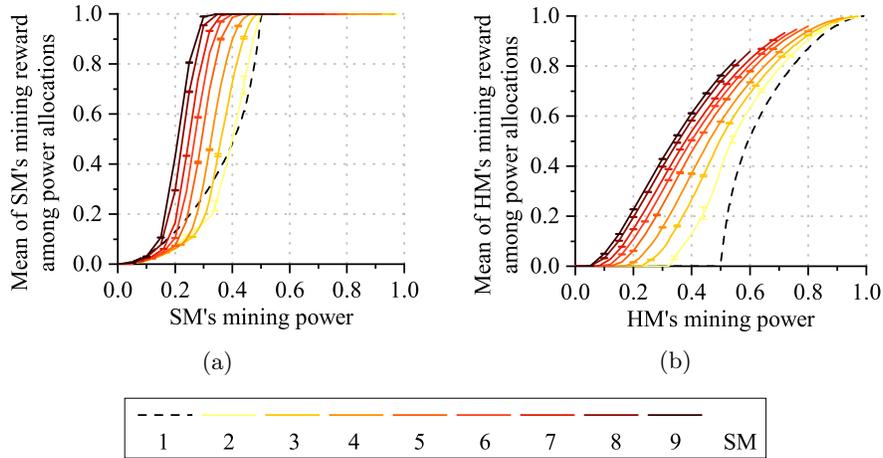


Fig. 1: Average of the SM’s mining reward among different power allocations with specific SM’s mining power (a) and an average of the HM’s mining reward among different power allocations with specific HM’s mining power (b) in a system with different numbers of SM. Standard error of the mean is shown as an error bar.

As shown by Liu et al. [10], our observation has also revealed a similar underlying cause of the trend of HM/SM’s mining reward. Generally, the higher the

number of miners, the less mining power each of them has. With a low mining power, SM is less likely to create a private chain longer than the other chains and therefore most of their computational resources are wasted. In turn, a mining power that HM/SM requires to earn an unfairly large mining reward become less in a system with a large number of miners.

Surprisingly, a number of SM miners can simultaneously get their unfairly large rewards under some specific power allocations. In particular, for each number of SM miners, their mining powers in such a power allocation are the same and also larger than a certain value. However, the range of such mining powers decreases and shortens as the number of SM increases as shown in Figure 2. We therefore hypothesise that this behaviour does not exist in a system with an extremely large number of miners.

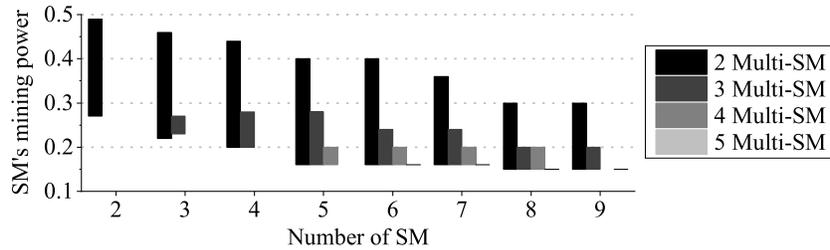


Fig. 2: Ranges of mining power of multiple and profitable SM (Multi-SM) with respect to an increasing number of SM. The number of Multi-SM indicates a number of SM miners who simultaneously gain a mining reward that is more than their mining power. In such ranges, the individual mining powers of the SM are equal.

5.2 Dynamic Strategy Mining

In the previous section, we have shown that a SM miner with low mining power earns less than their power. However, they might be able to earn more if they switch back to HM instead. Such a switch can induce further strategy switches due to a change in mining reward. In this section, we use a game-theoretical concept of equilibria (as described in Section 4) to tackle the strategy change and discuss the outcome.

We first notice multiple equilibria for particular power allocations and at least one equilibrium for every power allocation in every number of StrM in the system. As shown in Figure 3(a), the average number of ϵ -PE per power allocation is always at least one. However, it becomes extremely large in power allocations where there is a StrM with a relatively high mining power.

We observe that the large number of ϵ -PE is caused by a StrM miner expressing an indifference between HM and SM strategy where there is another StrM

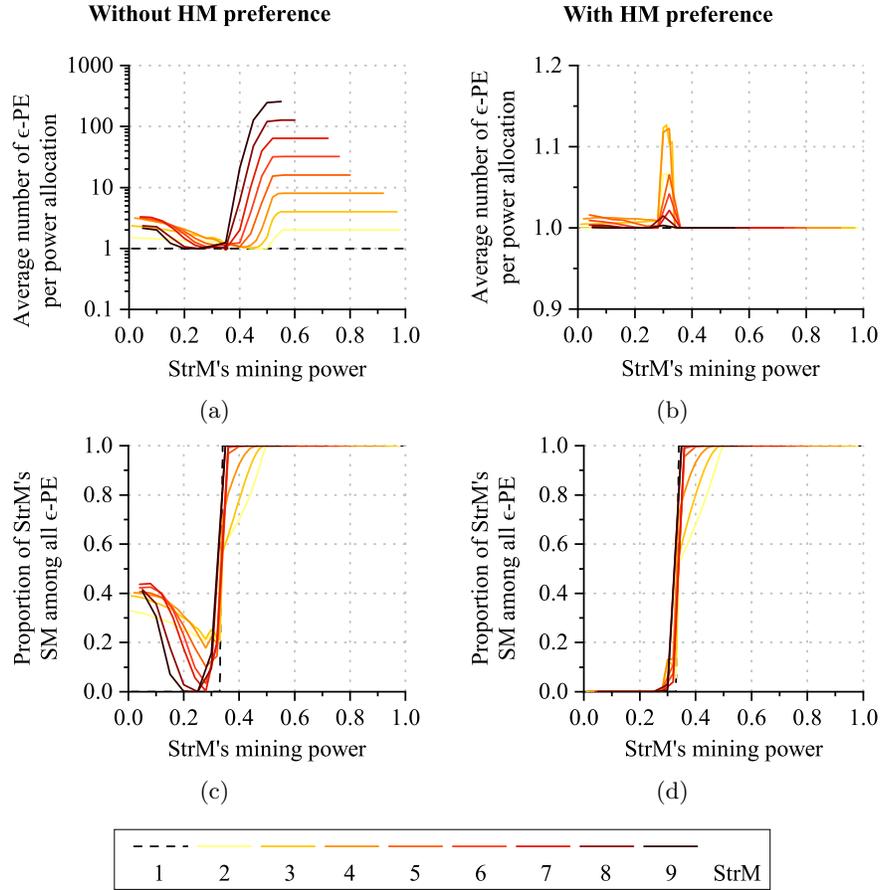


Fig. 3: Average number of ϵ -PE per power allocation (a,b) and an overall StrM's strategy in ϵ -PE (c,d) with different number of StrM in the system. Left figures (a,c) are results not under the HM-preference assumption, while right figures (b,d) are results under the HM-preference assumption.

with a particularly large mining power. In such a situation, there is no significant difference of mining reward between HM and SM used by the StrM with low mining power; which results in a moderate amount of StrM’s SM over all ϵ -PE as depicted in Figure 3(c). Consequently, the number of ϵ -PE will simply be a combinatorial number of the StrM’s HM/SM with low mining power and therefore grows in an increase of the number of StrM as shown in Figure 3(a).

With the HM-preference assumption, a reasonable choice of StrM’s strategy in ϵ -PE is obtained. In particular, StrM will no longer choose SM if there is no significant difference between HM’s and SM’s mining reward. The change of strategy in ϵ -PE is clearly demonstrated by a comparatively low average number of PSNE per power allocation in Figure 3(b) and no SM strategy chosen by StrM with mining power under 0.3 in Figure 3(d).

Clearly, StrM choose SM more than HM as their mining power increases to enjoy a larger amount of mining reward. This speculation is confirmed in Figures 3(d) and 4(a). That is, StrM starts to choose SM more once their mining power exceeds one-fourth. Once StrM possesses at least half of the total mining power, they always choose SM to earn the whole mining reward from the system.

Interestingly, the more StrM in the system, the more their choice of mining strategy and their mining reward becomes similar to the case of single StrM. As demonstrated in Figure 3(d), when the number of StrM miners increases, the transition of the StrM’s strategy from HM to SM gradually becomes sharper similarly to the case of single StrM. Likewise, Figure 4(a) shows a convergence of the mining reward of StrM with mining power lower than $\frac{1}{2}$ to one of the case of single StrM.

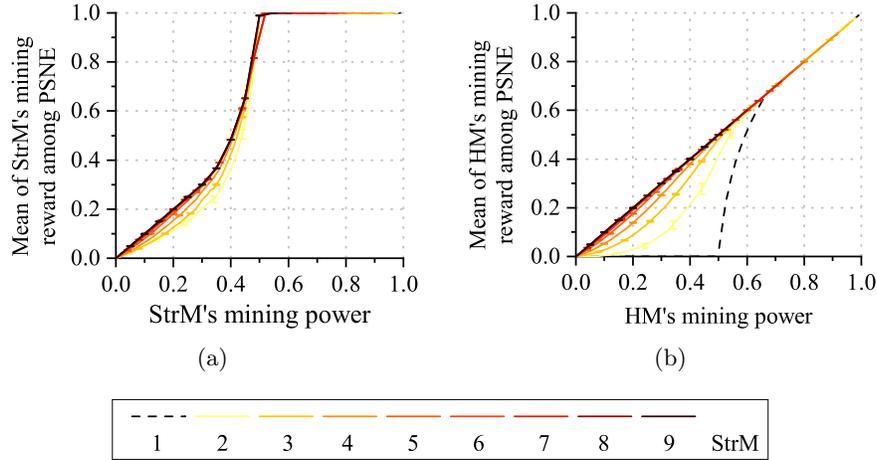


Fig. 4: Average of the StrM’s mining reward among different ϵ -PE with specific StrM’s mining power (a) and average of the HM’s mining reward among different ϵ -PE with specific HM’s mining power (b) in a system with different numbers of StrM. Standard error of the mean is shown as an error bar.

In contrast, the HM’s mining reward does not converge to one in the case of single StrM. Instead, it converges to their mining power as the number of StrM increases. This is empirically shown in Figure 4(b), where the mining reward of HM’s mining power under 0.67 asymptotically approaches their mining power as the number of StrM increases.

Even with the HM-preference assumption, there still are multiple ϵ -PE for particular power allocations. Such multiple equilibria are shown in Figure 3(b) where an average number of ϵ -PE per power allocation is more than one for any StrM’s mining power ranging up to 0.36. We found that multiple StrM with the same mining power larger than 0.3 together choose either HM or SM in such ϵ -PE. Since an individual deviation from HM to SM or vice versa yields a comparatively low mining reward for the deviating StrM, multiple ϵ -PE with such StrM together choosing HM or SM are formed.

On further inspection, the ϵ -PE where multiple SM are chosen by StrM becomes less likely to occur as the number of StrM increases. Compared to the fixed strategy model’s, the range of mining power of multiple SM in this model is even less. As shown in Figure 5, a mining-power range of multiple StrM miners that possess nearly equal power and together choose SM in ϵ -PE shortens in an increase of the number of StrM. Therefore, it is clear that this multiple SM is highly unlikely to occur in the presence of large number of StrM.

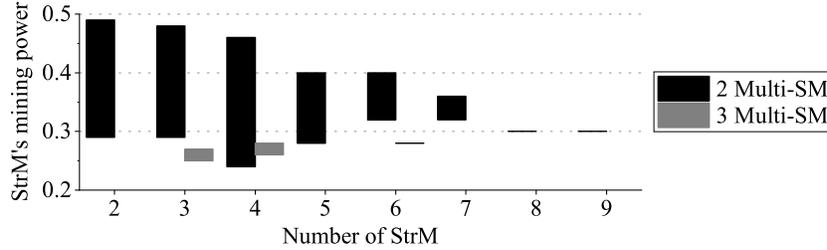


Fig. 5: Ranges of mining power of multiple and profitable SM (Multi-SM) with respect to an increasing number of StrM. The number of Multi-SM indicates a number of StrM miners who individually use SM and simultaneously gain mining reward more than their mining power. In such ranges, the individual mining powers of such StrM are equal.

5.3 Safety Level and Power Threshold

As shown in Figure 6, the safety level against SM/StrM monotonically decreases as the number of SM/StrM grows. Since the mining power that one miner possesses will decrease in an increasing number of miners in the system, SM/StrM with low mining power will become prominent. Such SM/StrM are unable to frequently create a private chain longer than the others (Section 5.1) and consequently choose HM to maximise their rewards (Section 5.2). As a result, the total

mining power of miners performing HM increases, and the HM miner requires less mining power to prevent SM/StrM.

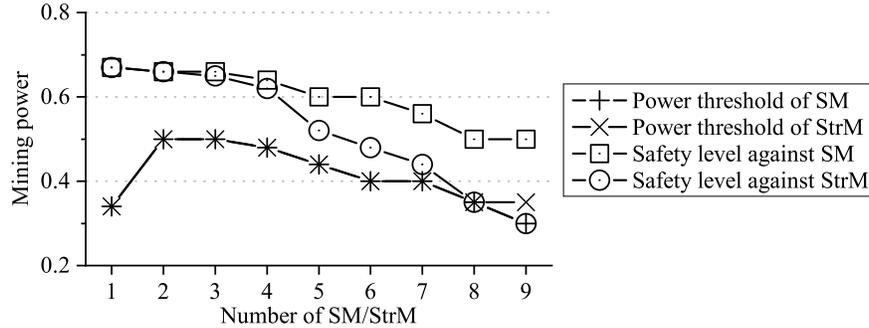


Fig. 6: Power thresholds and safety levels with respect to different numbers of SM/StrM in the system. No difference of a safety level between one with the HM-preference assumption and one without the assumption is found.

Moreover, the safety level is upper bounded by the case of one SM/StrM; that is, it is no greater than $\frac{2}{3}$. Intuitively, the case of one SM/StrM is the most difficult to prevent since it is a coalition of all SM/StrM miners combining their mining power and working together against HM miners. The safety level in this case is therefore the greatest one.

Similarly, the power threshold of SM/StrM decreases in an increasing number of SM/StrM after the case of single SM/StrM in the system. Due to SM with low mining power constantly wasting their effort, the amount of mining power which is required to secretly build the longest chain becomes less in turn.

However, the power threshold of StrM is strictly lower bounded at $\frac{1}{3}$. A similar rationale can be applied here: HM with a mining power of $\frac{2}{3}$ is the most difficult for SM strategy and therefore a mining power of $\frac{1}{3}$ is at least required. On the contrary, StrM with mining power lower than $\frac{1}{3}$ will always choose HM, as shown in Figure 3(d).

Clearly an upper bound of the power threshold of SM/StrM is $\frac{1}{2}$, which corresponds to Nakamoto’s analysis [11]. Any mining power beyond the threshold always allows SM/StrM to successfully create the longest chain.

6 Conclusions and Future Work

In this work, an empirical investigation of the Selfish Mining (SM) strategy employed by multiple miners has been carried out. We separately considered two types of malicious miners where one (SM miner) always follow SM and the another (StrM miner) chooses to follow either Nakamoto’s mining protocol or the SM strategy depending on which maximises its mining reward. Since our

work accounted for multiple miners and a large number of malicious miners in the system, our findings (such as the case of multiple miners simultaneously and individually performing SM) are more practical than the other's so far.

The effectiveness of the SM strategy varies when different types and different numbers of malicious miners are considered. In general, SM is more effective in the presence of a large number of SM miners since it can reap a larger amount of mining reward with the same hash rate in a system with StrM miners. However, SM in a system with a low number of StrM miners is less effective than one in a system with SM miners since it yields a smaller mining reward with the same hash rate.

Regardless of the type and the number of miners in the system, the least hash rate to perform SM and to prevent SM are no greater than $\frac{1}{2}$ and $\frac{2}{3}$ respectively. Additionally, both amounts of hash rate monotonically decrease in an increase of the number of malicious miners in the system. If only StrM miners are considered, then the least hash rate required for SM is strictly $\frac{1}{3}$. However, such an amount reduces further than $\frac{1}{3}$ (as originally reported by Eyal and Sirer [6]) if SM miners are considered.

Despite the aforementioned, our result suggests that PoW blockchain systems are required to have a large number of miners to be more secure against SM. Since blockchain miners are working to earn their mining reward, they are utility-maximising agents or StrM miners in our model. As shown in Section 5.2, SM is comparably less chosen in the presence of a large number of StrM miners. Together with the decreasing hash rate required for preventing SM, it can be concluded that a large number of miners can prevent SM and possibly similar malicious mining strategies.

A number of interesting questions still remain to be further investigated. As pointed out by Eyal and Sirer [6], a network capability of SM miners is also an important factor that affects the effectiveness of SM. This aspect will be taken into account in our future work. Moreover, an optimal SM strategy in the context of multiple miners, similar to that in the work of Sapirshtein et al. [13], is not yet known. With the optimal strategy, it remains to be seen whether our findings are still valid.

Acknowledgement The authors gratefully acknowledge financial support from the EPSRC Doctoral Training Partnership, and the use of IRIDIS High Performance Computing Facility at the University of Southampton. We also would like to express our gratitude to all anonymous reviewers for their insightful comments.

References

1. Azaria, A., Ekblaw, A., Vieira, T., Lippman, A.: Medrec: Using blockchain for medical data access and permission management. In: 2016 2nd International Conference on Open and Big Data. pp. 25–30 (2016)

2. Bitcoin Wiki: Mining (2018), <https://en.bitcoin.it/wiki/Mining>, Accessed: 1 Jul 2019
3. Bitcoin Wiki: Pooled mining (2018), https://en.bitcoin.it/wiki/Pooled_mining, Accessed: 14 Jun 2019
4. Bitcoin Wiki: Block (2019), <https://en.bitcoin.it/wiki/Block>, Accessed: 13 Jun 2019
5. Christidis, K., Devetsikiotis, M.: Blockchains and smart contracts for the internet of things. *IEEE Access* **4**, 2292–2303 (2016)
6. Eyal, I., Sirer, E.G.: Majority is not enough: Bitcoin mining is vulnerable. In: Christin, N., Safavi-Naini, R. (eds.) *Financial Cryptography and Data Security, FC 2014, Lecture Notes in Computer Science*. vol. 8437, pp. 436–454. Springer, Berlin, Heidelberg (2014)
7. Gervais, A., Karame, G.O., Wüst, K., Glykantzis, V., Ritzdorf, H., Capkun, S.: 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. CCS '16, ACM, New York, NY, USA (2016)
8. Göbel, J., Keeler, H.P., Krzesinski, A.E., Taylor, P.G.: Bitcoin blockchain dynamics: The selfish-mine strategy in the presence of propagation delay. *Performance Evaluation* **104**, 23–41 (2016)
9. Kiayias, A., Koutsoupias, E., Kyropoulou, M., Tselekounis, Y.: Blockchain mining games. In: Conitzer, V., Bergemann, D., Chen, Y. (eds.) *Proceedings of the 2016 ACM Conference on Economics and Computation, EC '16*. pp. 365–382. ACM Press, New York, USA (2016)
10. Liu, H., Ruan, N., Du, R., Jia, W.: On the strategy and behavior of bitcoin mining with n-attackers. In: *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*. pp. 357–368. ASIACCS '18, ACM, New York, NY, USA (2018)
11. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system (2008), <https://bitcoin.org/en/bitcoin-paper>, Accessed: 28 Nov 2015
12. Nayak, K., Kumar, S., Miller, A., Shi, E.: Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. In: *2016 IEEE European Symposium on Security and Privacy*. pp. 305–320. IEEE Press, Los Alamitos, US (2016)
13. Sapirshtein, A., Sompolinsky, Y., Zohar, A.: Optimal selfish mining strategies in bitcoin. In: Grossklags, J., Preneel, B. (eds.) *Financial Cryptography and Data Security, FC 2016, Lecture Notes in Computer Science*. vol. 9603, pp. 515–532. Springer, Berlin, Heidelberg (2017)
14. Wood, G.: Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper* **151**, 1–32 (2014)
15. Zhang, R., Preneel, B.: Publish or perish: A backward-compatible defense against selfish mining in bitcoin. In: *Topics in Cryptology, CT-RSA 2017, Lecture Notes in Computer Science*. vol. 10159, pp. 277–292. Springer, Cham, Switzerland (2017)
16. Zyskind, G., Nathan, O., Pentland, A.: Decentralizing privacy: Using blockchain to protect personal data. In: *2015 IEEE Security and Privacy Workshops*. pp. 180–184 (2015)