Mining blocks in a row: A statistical study of fairness in Bitcoin mining

Sheng-Nan Li
URPP Social Networks
University of Zurich
CH-8050 Zurich, Switzerland
shengnan.li@uzh.ch

Zhao Yang
URPP Social Networks
University of Zurich
CH-8050 Zurich, Switzerland
zhao.yang@business.uzh.ch

Claudio J. Tessone
UZH Blockchain Center, URPP Social Networks
University of Zurich
CH-8050 Zurich, Switzerland
claudio.tessone@business.uzh.ch

***Abstract*—The Bitcoin system keeps its ledger consistent in a blockchain by solving cryptographic problems, in a method called "Proof-of-Work". The conventional wisdom asserts that the mining protocol is incentive-compatible. However, Eyal and Sirer in 2014 have discovered a mining attack strategy called selfish mining (SM), in which a miner (or a mining pool) publishes the blocks it mines selectively instead of immediately. SM strategy would have the impact of wasting resources of honest miners. Scholars proposed various extensions of the SM strategy and approaches to defense the SM attack. Whether selfish mining occurs in practice or not, has been subject of extensive debate. For the first time, in this paper we propose a method to identify selfish miners by detecting anomalies in the properties of consecutive blocks' statistics. Furthermore, we extend our method to detect the mining cartels, in which miners secretly get together and share timely information. Our results provide evidence that these strategic behaviors take place in practice.**

***Index Terms*—Bitcoin, Selfish Mining, Mining Cartel, Consecutive Blocks' Statistics**

I. Introduction

Blockchains, decentralized techno-economic systems, store verified data in blocks of a chain and secures data transmission away from manipulation using cryptography [1]. Among all the blockchain-based ecosystems, Bitcoin is the most famous one. The central part of Bitcoin is the public, permissionless blockchain. The consistency of data storage is maintained by all participants solving hash puzzles, which also called *mining blocks*. In order to solve the puzzle, attempts have to be made through brute force, and therefore, *a priori*, the probability of finding a solution is proportional to the number of tries per unit of time each miner is able to perform. Each miner will be rewarded by a nominal amount of Bitcoin if he is the first acknowledged miner to find a valid block, which extends the longest chain in the network. This kind of Proof-of-Work (PoW) consensus is employed in almost 90% of public blockchains [1]. According to this mechanism, the more mining power (or resources) a miner invests, the larger are his chances to solve the puzzle first [2]. Thus, miners often join in mining pools to share their revenue relying on larger mining power. This type of rewarding system provides an incentive for miners to contribute their resources to the system, and is essential to the currency's decentralized nature.

978-1-7281-6680-3/20/$31.00 ©2020 IEEE

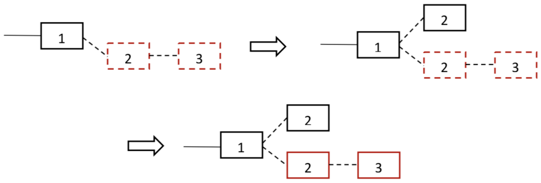

Fig. 1. An example event of selfish mining strategy

However, in 2014 Eyal and Sirer [3] discovered a mining attack strategy in Bitcoin, called *selfish mining* (SM). They described the SM strategy as follows: "The selfish mining pool keeps its mined blocks private, secretly forking the blockchain and creating a private branch; then selfish miner judiciously reveals blocks from the private branch to the public, such that the honest miners will switch to the recently revealed block, abandoning the shorter public branch. This renders honest miner's previous effort spent on the shorter public branch wasted". When implementing the SM strategy, selfish pools make decisions on whether to publish their mined block or not based on the relative lengths of their private branch versus the public branch. Take one event as an example, as shown in Fig. 1. When a selfish pool holds a lead of two blocks (in red), it will continue to mine at the head of its private branch. Once the honest miners publish a new block that reduces selfish pool's lead to only one block, selfish pool will immediately publish its secret blocks. Since the previously private branch is longer, the selfish pool obtains the revenue of these two blocks. Eyal and Sirer [3] also claimed higher revenues will lead more miners to join the selfish pool, a dangerous dynamic to the decentralization of cryptocurrency ecosystem.

The theory of SM attack has drawn a lot of attention and many extended SM strategies have been proposed [4], such as stubborn mining, and publish-n strategy [5]–[7]. Scholars also proposes various defense in accordance with the attack strategies. Existing defenses can be categorized into two approaches: making fundamental changes to the block validity rules, or lowering the chance of honest miners working on the selfish miner's chain during a forked situation, such as *ZeroBlock* [8], a timestamp-free solution, which requires that each block must be generated and received by the network within a maximum acceptable time interval, and *weighted FRP* [9], which asks miners to compare the weight of the chains instead of their length. In addition, there are some researches about whether SM strategy could be profitable for selfish miners: Some studies indicated that SM may let attacker gain extra revenue and break the balance between revenue and mining power [4], while some scholars argued that selfish miners can never earn more revenue but only put themselves at risk for no gain [10].

Although the market capitalization of cryptocurrencies has increased tremendously in the last years, and a previous study [3] in Bitcoin has claimed that "mining pools have been benign and followed the protocol so far", there is still a lot of discussion about whether some miners are actually behaving against the mining protocols. In this paper, we try to answer this question through an empirical analysis of the Bitcoin system.

To the best of our knowledge, our empirical analysis of the SM attack in the Bitcoin system is presented for the first time. Ignoring the controversial influence of SM strategy on the amount of miners' revenue, we sue the fact that selfish miners' behavior of selectively revealing his mined blocks would cause abnormal probability of consecutively mining two blocks. Based on this insight, we propose an identification method of SM behavior by quantifying miners output of mining blocks continuously. Furthermore, we extend our method to identify the mining cartels, in which miners secretly get together and share timely information related to the blocks mined.

II. Dataset and Method

A. Dataset

The Bitcoin network was started on 3rd Jan. 2009 when the internet persona Satoshi Nakamoto mined the first block of the chain, known as the genesis block. Our dataset contains blocks mined from January 2009 to September 2019, including blocks' height, mined time, the corresponding miners, etc. The mining addresses whose identity cannot be traced back to a known entity are labelled as "Unknown". The number of blocks and named mining pool during each month are shown in the Fig. 2. One can find that from January 2012 on, as a result of the difficulty adjustment in Bitcoin mining protocol, the number of the blocks in every month is relatively stable. The maximum number of named mining pool is 31 at March and April in 2017. In addition, the revenue share among named mining pools and "Unknown" miner is shown in Fig. 3.

It is worth to mention that the fraction of blocks mined by unknown mining addresses has decreased over time. Although some of the unknown mining addresses might be owned by named pools (e.g. to hide their activities such as selfish mining), one can easily observe that more and more rewards were gained by named pools - actually over 99% of blocks are mined by named pools between September 2015 and February 2016.

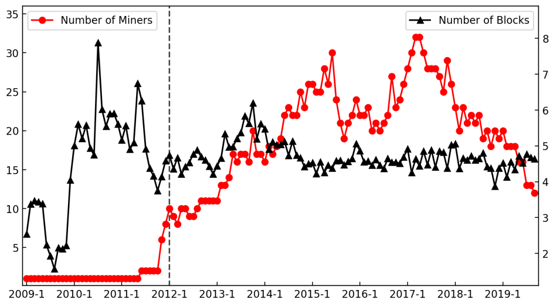

Fig. 2. Monthly number of miners and blocks in Bitcoin

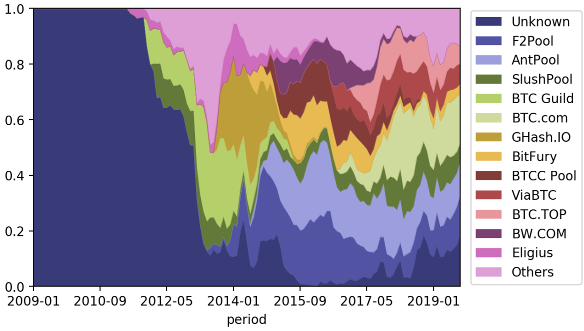

Fig. 3. Monthly revenue share among miners in Bitcoin

B. Identification Method of Selfish Miner

According to the Bitcoin protocol, the fair proportion of blocks a miner may discover during a time period(revenue share) is equal to his devoted mining power (number of attempts to solve the puzzle) divided over the total mining power of the network. In this idealized view, the discovery of each block is random and independent without influence from the previous blocks, because the information diffuses through the network instantaneously [11], [12]. Thus, it is reasonable to assume that during a certain time period there exists an expected number of blocks that one miner can discover (which is proportional to the miner's mining power), while the order of miners who mined blocks in this period should be random. When doing an SM attack, however, the selfish miners selectively publish their mined blocks. This, should lead to an identifiable increase in their chances of discovering two blocks consecutively (although it may not significantly increase either the amount or the proportion of blocks mined by selfish miners during that time period [10]).

In this study, we propose an identification method that controls the amount of blocks mined by each miner, and then repeatedly shuffles the order of miners' discoveries of these blocks in each time period. This method could provide the distribution and the expected value of times that each miner could continuously discover two blocks. In the t-th shuffle round, the number of times that miner i continuously mines two blocks during period T is denoted as $S_i^T(t)$.

We perform a bootstrap analysis of the mining output of each miner i by comparing the actual times C_i^T that miner i

continuously discover two blocks in the time period T with the expected times $S_i^T(t)$ from the reshuffled simulation. The measurement of miner's mining behaviors be can be defined as:

$$SM_i^T = \frac{C_i^T - \langle S_i^T(t) \rangle}{\sigma\left[S_i^T\right]} \tag{1}$$

where $\langle S_i^T \rangle$ and $\sigma\left[S_i^T\right]$ are the expected value and the standard deviation of all the observations $S_i^T(t)$, respectively. In order to identify miners with different level of abnormal in doing SM, we set a criterion for our method. In details, when we set the criterion as $SM > 2$ (with a confidence of 95%), it means that any miner whose SM_i^T value of a certain month T exceeds 2 will be identified as a selfish miner by our method.

III. Results

A. Mining Behaviors of Miners in Bitcoin

In this study, we focus on the period after January 2012 in Bitcoin when the number of the blocks in every month is relatively stable. We have conducted 1000 times shuffle simulations of block mining during each month. The monthly SM values of mining pools in Bitcoin are shown in Fig. 4. We have noticed that some miners with less revenue shares during a month might has a larger SM values. After determining the criterion for identification method, we will be able to label the selfish miners. According to Fig. 4, when we set the criterion for identifying the selfish miners as $SM > 2$, the largest revenue share of selfish miners is about 25%. And when we set the criterion as $SM > 3$, the largest revenue share of selfish miners is less than 15%.

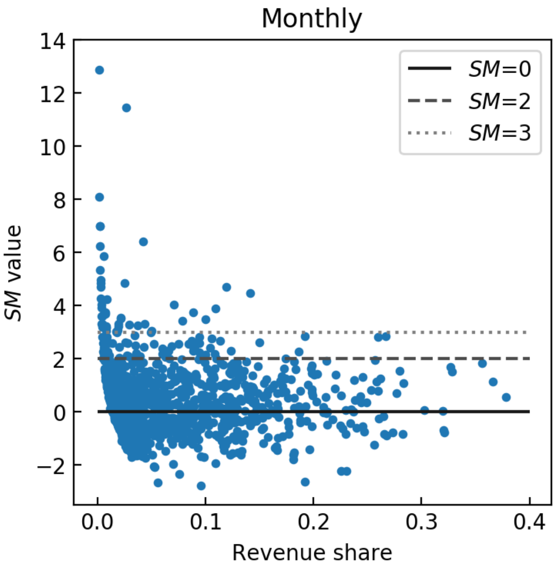

Fig. 4. Monthly SM values of miners corresponding with their monthly revenue share.

B. Identified Selfish Miner

Under the criterion $SM > 2$, the detected selfish miners in Bitcoin are shown in Fig. 5, where the miners are ranked by the number of times they have been identified. In Fig. 5, we only displayed miners who have been identified at least 4 times during each month in Bitcoin. The empirical results show that the SM strategy might have been implemented by several miners in Bitcoin system.

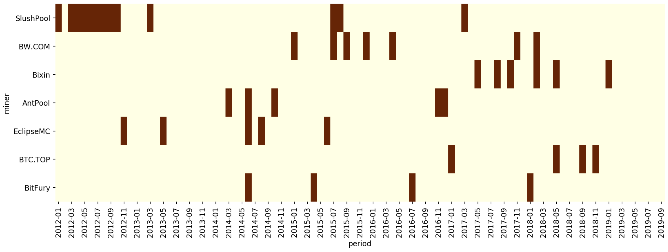

Fig. 5. The identified selfish miners of each month in Bitcoin

IV. Mining Cartel

A. Identification Method of Mining Cartel

From the results of section III, we have noticed that the SM strategy is employed mainly by miners with less revenue share, and the identified selfish miners might not continuously behave in SM strategy. However, if miners secretly built a cartel, participants of the cartel will benefit from the huge mining power, as well as the information of blocks mined by the other members. Therefore, in this part, we would like to verify if mining pools have formed secret cartels. we have extended our identification method from single mining pool to pairs of mining pools (i.e. paired shuffle simulation). When doing the paired shuffle simulation, the measurement of identification of mining cartel can be defined as:

$$MC_{ij}^T = \frac{C_{ij}^T - \langle S_{ij}^T \rangle}{\sigma\left[S_{ij}^T\right]} \tag{2}$$

where C_{ij}^T is the actual times that two consecutive blocks are first mined by miner i, then by miner j. S_{ij}^T is the observed value of each shuffle round that the number of times that two consecutive blocks are first mined by miner i, then by j during period T. $\langle S_{ij}^T \rangle$ and $\sigma\left[S_{ij}^T\right]$ are the corresponding expected value and the standard deviation, respectively.

B. Identified Mining Cartel

We calculate the MC value of each pair of miner pools on a monthly level. After determining the criterion of the paired shuffle simulation for identifying mining cartel as $MC > 2$, we label pairs of miners whose MC values are larger than 2 as a mining cartel during each month. The number of times that each pair of miners is labeled as a mining cartel are shown as Fig. 6. The miners are ranked by the sum of times they are identified as a member in a cartel. And we only show the mining cartels among the top 50 abnormal miners. For instance, the "BitMinter-F2Pool" pair has been detected as a mining cartel for 6 times. We have noticed that miners might build the mining cartels with different miners. Besides, some abnormal mining pools that can not be identified in our first study do participant in cartels.

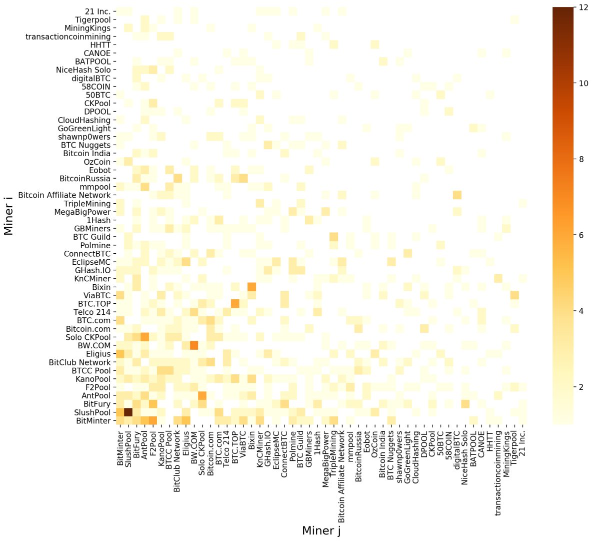

Fig. 6. Mining cartels among different mining pools

V. Conclusion

The cryptocurreny, as a decentralized ecosystem, is maintained through distributed consensus. Given the fact that the blockchain users typically do not trust each other, enabling fairness in the existing cryptocurrencies is fundamental. There have been many studies about consensus mechanisms that secure and embed trust in systems, as well as studies about the attacking strategies that destroy it. To our knowledge, most of the previous studies are analytical models that focus on the cost-benefit analysis, while the empirical and quantitative researches are rare. In this study, we have conducted empirical analysis of mining behaviors in the most famous "Proof-of-Work" based cryptocurrency, Bitcoin. We detect miners' anomalies based on the properties of consecutive blocks' statistics.

In the first study, we have identified several mining pools with abnormally high success rate of continuously discovering two blocks. We believe that the reason for some mining pools' abnormality is because they are using selfish mining strategy, however finite diffusion block time in the network [11] could also be an explanation. In addition to that, our result also shows that the SM strategy are more popular in miners with smaller revenue share, and the identified selfish miners do not continuously employ the SM strategy.

In the second part of this study, we are interested in detecting the mining cartels. We extended our method from including a single mining pool to a pair of mining pools, and have observed that the mining cartels do exist in Bitcoin. We have also noticed that some selfish mining pools that cannot be identified in the first study are actually participating in the mining cartels. We would like to point out that the existence of mining cartels has been ignored in many previous studies. The conventional wisdom believes that the mining protocol is secure as long as the pool's mining power is limited in certain threshold. However, these assessments are based on the condition that the mining pools are operating independently. In theory, miners or mining pools could make secret cartels, which may cause the threat to the security of blockchain-based systems.

There are some limitations in our work: First of all, we have limited our analysis to the simplest case of mining blocks consecutively, which is two blocks. An analysis of three or more blocks would provide more insights. Second, we have proposed that the selfish mining attack and the existence of mining cartels are two possible reasons of the abnormal high continuously succeed rate. However, there could be some other explanations (like finite diffusion times).

In the end, we stress that this study contributes to both research and practice. In terms of research, we have highlighted the importance of conducting empirical analyses when investigating the fairness of blockchain-based ecosystems: mathematical or economical models that focus on the cost-benefit analysis are not suitable as participants of cryptocurrencies might have bounded rationality or be risk seeking. In terms of practice, we have provided actual and simple techniques to identify suspicious participants. Our next step is to analyze the fairness of different cryptocurrencies. Our methods may also be applied as a forensics tool to identify other abnormal mining behaviors, for instance, cheat by changing addresses.

References

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

[2] S. Nakamoto *et al.*, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[3] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in *International Conference on Financial Cryptography and Data Security*, pp. 436–454, Springer, 2014.

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

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

[6] Q. Bai, X. Zhou, X. Wang, Y. Xu, X. Wang, and Q. Kong, "A deep dive into blockchain selfish mining," in *ICC 2019-2019 IEEE International Conference on Communications (ICC)*, pp. 1–6, IEEE, 2019.

[7] H. Liu, N. Ruan, R. Du, and W. Jia, "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, ACM, 2018.

[8] S. Solat and M. Potop-Butucaru, "Brief announcement: Zeroblock: Timestamp-free prevention of block-withholding attack in bitcoin," in *International Symposium on Stabilization, Safety, and Security of Distributed Systems*, pp. 356–360, Springer, 2017.

[9] R. Zhang and B. Preneel, "Publish or perish: A backward-compatible defense against selfish mining in bitcoin," in *Cryptographers' Track at the RSA Conference*, pp. 277–292, Springer, 2017.

[10] C. S. Wright and S. Savanah, "The fallacy of the selfish miner in bitcoin: An economic critique," 2017.

[11] C. Decker and R. Wattenhofer, "Information propagation in the bitcoin network," in *IEEE P2P 2013 Proceedings*, pp. 1–10, IEEE, 2013.

[12] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain," in *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pp. 2567–2572, Oct 2017.