On the Instability of Bitcoin Without the Block Reward

Purpose of the study

Bitcoin has a policy that causes the block reward to halve after every 210,000 blocks are mined.

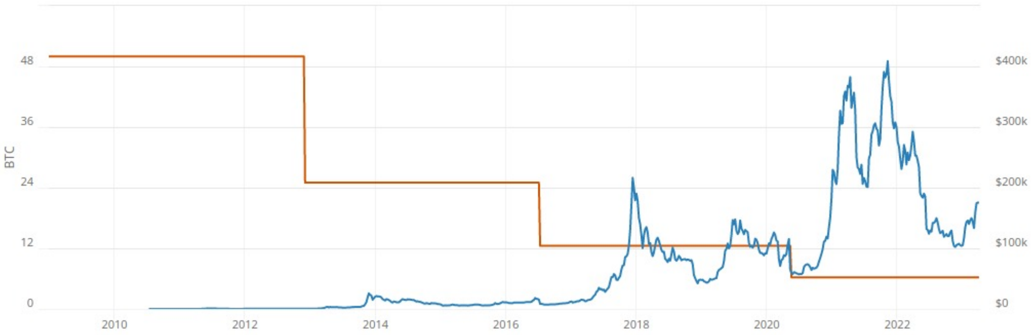


Figure 1: Block rewards of Bitcoin (orange line) [1].

The orange lines show how the block rewards have reduced after each halving event. Eventually, the block rewards will become zero and transaction fees will be the only incentive for the miners. It has been believed that in both cases, the miners have an equal incentive to mine honestly. This paper shows that it is not true. When the block rewards disappear, the transaction fees model of Bitcoin will lead to many dishonest miners.

Unlike the constant block reward, the transaction fees vary a lot. Miners will adopt various dishonest strategies to maximise their revenue. This can be a threat to the security and stability of the block chain.

Methods

The study is done using a game-theoretic framework. The block reward is 0 and the only rewards for the miners are the transaction fees.

The mining is formulated as a ’game’ in which the miners are playing/learning by a no-regret learning algorithm [2]. It essentially means that their rewards will at least be as good as the rewards of the best strategy. Using this technique, they will be able to achieve a steady state which is profitable for them. This proves that the miners have an incentive to use the proposed dishonest strategies.

The authors have proved that the new dishonest mining strategies are indeed profitable in the long run using the notion of equilibrium. They have shown that when all or some percentage of miners adopt a certain dishonest strategy, the system reaches an equilibrium which is profitable to the dishonest miners. At the same time, it is not rewarding to the few honest miners. It is also a threat to the stability and security of the Bitcoin block chain.

In addition to proving that an equilibrium exists, the paper simulates the strategies on a mining simulator [1]. This tool shows that the theoretical results are valid and the system will actually reach an equilibrium. Theory proves that an equilibrium exists, and the simulator helps to verify it. Hence, theory and simulation complement each other in this study.

Novelties

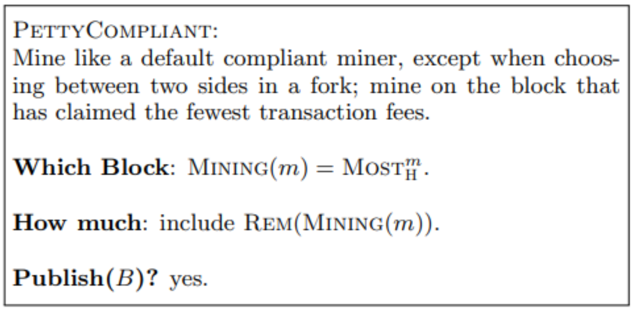
1. A mining simulator: To make the conclusions of the paper more intuitive and understandable, a mining simulator has been provided. It is written in C++ and doesn’t require high system specifications. It is fast and can run 1000 games with 200 miners in a few seconds. It has a set of customizable parameters that can be used to simulate multiple mining strategies.

[1] https://github.com/citp/mining

The simulation results have been used extensively to verify the theoretical results obtained in this paper. Hence, it is very novel and useful.

2. Well-defined terminology: To outline the various strategies and results of the game-theoretic framework, it is important to have a clear set of terms. The paper manages to achieve that by introducing a well-defined terminology. For example, the paper introduces terms to refer to the oldest mined block, the remaining transactions, the height of the block, etc. It also puts miners into two categories - atomic and non-atomic, depending on how they strategise. The mining strategies have been described with the help of succinct terms such as continuing [2] and undercutting [3].

The deviant miner strategies are modeled by a set of decisions they make, and these decisions can be used to formulate a strategy in a very concise way.



PETTYCOMPLIANT:
Mine like a default compliant miner, except when choosing between two sides in a fork; mine on the block that has claimed the fewest transaction fees.

Which Block: $\textsc{Mining}(m) = \textsc{Most}^{m}_{\mathrm{H}}$.

How much: include $\textsc{Rem}(\textsc{Mining}(m))$.

Publish(B)**?** yes.

Figure 2: An example of mining strategy.

3. New mining behaviours: The paper lays out three novel mining strategies for the transaction fee model of Bitcoin: (i) Petty compliance, (ii) Lazy undercutting, and (iii) Aggressive undercutting. Petty compliant miners are miners that always build upon the block that gives them the highest rewards. Note that it is different from the default strategy that always extends the longest chain.

Undercutting takes advantage of the presence of petty compliant miners. An undercutting miner will fork the block chain and claim the transaction fees. Then, they incentivize the petty compliant miners by leaving a high reward to be claimed. Hence, those miners will build upon the forked block and ignore the original longest chain.

These mining behaviors can be simulated to see that the system does arrive at an equilibrium in presence of dishonest miners.

4. A sophisticated selfish mining strategy: Picking up from the selfish mining strategy discussed in a related work [3], the authors go on to propose a more powerful strategy. They also prove that selfish mining strategy works even better in their transaction fee model.

A selfish miner doesn't publish a block that they've mined and lets other miners waste their computation power mining for a new block. When a block is published, the selfish miner orphans that block by publishing the block they had found. This increases their hash power share and hurts other miners. The proposed improved selfish mining strategy works by being more reasonable about which blocks to withhold and which ones to publish immediately.

The authors have concluded that a selfish mining strategy is immediately profitable in the transaction fee model. In the related work [3], the selfish mining strategy takes some time before it becomes profitable. By deriving the reward equations for the improved selfish mine strategy and running simulations on the mining simulator, they have provided a sound reasoning to their claims.

[2] extending on the latest published block

[3] forking the block chain and extending the parent of latest block

Limitations

1. Simulator limitations: The mining simulator cannot simulate the case where transactions don't arrive at a constant rate. In real life, the number of transactions per unit time varies widely. Figure 3 shows how the number of Bitcoin transactions per day has varied over the past 3 years.

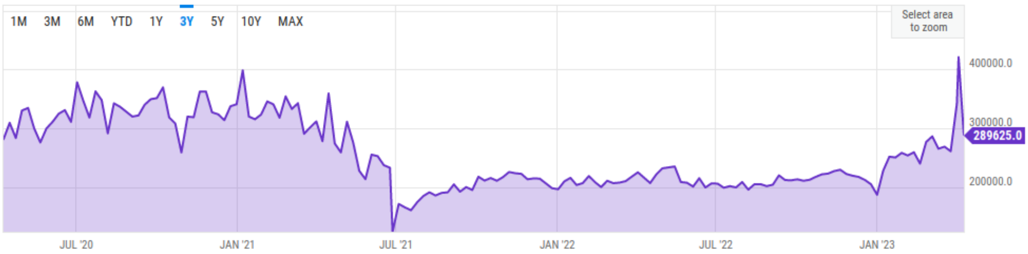


Figure 3: Transactions/day for past 3 years. [4].

While this assumption doesn't affect the validity of claims in the paper, it doesn't show the true picture about the transaction fees dynamics of Bitcoin.

The simulator also doesn't consider the presence of mining pools [4]. The simulator can be configured in a way that it represents a mining pool as a single miner with some hash power. But it cannot be shown exactly how the miners will behave when they have to be part of a pool and divide the rewards with other members of the pool. Pool-hopping [5] cannot be simulated either.

2. Simplifying assumptions: The authors make a set of assumptions that are very helpful in understanding the logic behind their claims. But, these assumptions also make the study far from reality. For example, the miners are assumed to take only three decisions when they are mining: which block to extend, which transactions to include, and whether to publish the new block or not. In real life, the miners take decisions based on a more complex thought process. What if the miner doesn't want to risk losing the rewards by acting dishonestly? The authors have built upon a negative point of view and have failed to consider this.

3. No communication among the miners: The authors have concluded that an equilibrium exists if all the miners are using the same undercutting strategy. But, there is no way to make sure that the miners actually do so. The miners aren't communicating to agree on a strategy. One result says that even if 66% of the miners are behaving honestly, undercutting will be profitable. Again, it is going to be difficult for other miners to know what percentage of miners are honest. It is a risk to undercut without an assurance of profit.

4. Limited state transition function: In the study of selfish mining strategies in a related paper [3], Markov decision process (MDP) has been used. In MDP, the miner moves in a discrete state space. This works fine in the block reward model because the block rewards of Bitcoin are discrete (6.25 BTC currently). But in the transaction fee model, the reward states are not discrete because transaction fees can take any real number value. As a result, they cannot be studied with MDP.

Despite this, the authors have used a discrete state space and MDP to derive results from the selfish mining strategy without much justification. It makes the credibility of results very questionable.

[4] a set of miners who mine together and divide their rewards in proportion of their hash powers

[5] miners going from one pool to another

Results of the study

1. Block reward is integral to the stability of any cryptocurrency. Maintaining an honest incentive for miners without a constant reward model is proved to be difficult.

2. In the absence of block rewards, the stability of Bitcoin is in danger. It leads to deviant mining strategies. Petty compliance, undercutting and selfish mining lead to an undesirable and insecure state of Bitcoin.

3. Undercutting attacks will cause dishonest miners to increase their hash power. They will extend only their own blocks. Hence, a transaction fee model will be vulnerable to 51% attacker and double spend attacks.

4. The dishonest miners can profit even if at most 66% of miners are honest. This is an unfavorable situation for the honest miners. Eventually, they might decide to leave the Bitcoin ecosystem.

Scope for future studies

A merit of this paper is that it provides enough solid foundation on which further research can be carried out.

For example, the mining simulator has several configurable parameters that can be tuned to explore more strategies.

The miner behavior can be studied in more detail by adding more conditions to their decision-making process. Undercutting strategies can be explored at heights lower than $H-1$ and so on. Here, H is the height of the latest published block.

The transaction arrival rate can be tweaked to see how it affects the mining strategies.

Essentially, this paper has created a good groundwork for further research. It has established terms and defined all the basics.

Concluding remarks

This research uncovers the possible dangers of the current Bitcoin model. If the block rewards become 0, the only remaining incentive will be the transaction fees. This is a complex situation which can lead to various outcomes. According to the paper, it will lead to a state where dishonest miners are present. The Bitcoin model will fail to stay profitable for the honest miners.

The authors haven't provided concrete solutions to the problems that can arise. But, it is not the goal of this study. They've also admitted that this paper is only a glimpse of the things that could go wrong.

Some newer cryptocurrencies have an even faster halving rate than Bitcoin. They are unaware of the problems it may cause in the long run. The authors suggest that making the block reward permanent is beneficial. It could be costly, but it would ensure the stability of the currency.

References

[1] *Block reward Per Block Chart*. `https://bitcoinvisuals.com/chain-block-reward`. 2023.

[2] Geoffrey J. Gordon, Amy Greenwald, and Casey Marks. “No-Regret Learning in Convex Games”. In: *Proceedings of the 25th International Conference on Machine Learning*. ICML ’08. Helsinki, Finland: Association for Computing Machinery, 2008, pp. 360–367. ISBN: 9781605582054. DOI: `10.1145/1390156.1390202`. URL: `https://doi.org/10.1145/1390156.1390202`.

[3] Ittay Eyal and Emin Gun Sirer. *Majority is not Enough: Bitcoin Mining is Vulnerable*. 2013. arXiv: `1311.0243 [cs.CR]`.

[4] *Bitcoin Transactions Per Day*. `https://ycharts.com/indicators/bitcoin_transactions_per_day`. 2023.