Game Theoretical Analysis of Selfish Mining in Blockchain

Zerui Cheng

Institute for Interdisciplinary Information Sciences
Tsinghua University

February 25, 2022

Overview

- This project is conducted under the supervision of Prof.Zhixuan Fang from Oct 2020 to May 2021, and this is my initial step into the area of research.
- In this project, we analyze the scenario where multiple self-interest-driven malicious miners conduct selfish mining in a Bitcoin system.

Background and Motivation

- I.Eyal, E.Sirer: **Majority is not enough: Bitcoin mining is vulnerable**
- In this paper, a new attack to Bitcoin named "Selfish Mining" was put forward, where a mining pool doesn't need as much as more than half of the computation power to gain more profit than honest mining.
- Suppose the network condition is equal for every agent, one only needs around 26% of total mining power to gain by more profit by unilateral deviation to selfish mining.
- However, in this paper, the authors only analyze the situation where only one miner deviates and other miners remain honest. And we're interested in the situation where multiple miners do selfish mining and the state of equilibrium.

Basic Modeling

What the miners do actually

When multiple selfish miners misbehavior, they compare their unpublished chain with the current longest published chain, and apply the same algorithm as mentioned in the paper, which will probably lead to a cascading block releasing process.

Analysis of the process

From simple derivation, after one honest miner publishes a block, a cascading block releasing will begin, where the selfish miner with the longest private chain will get admitted unless none of the selfish miners have mined a block, with $max(0, len_{max} - len_{max_2})$ (len_{max} denotes the longest private chain and len_{max_2} denotes the second longest private chain) blocks left in the winners' private chain (others' private chain will be cleared for sure).

Simplification

Simplification of the Modeling

For simplicity, here we accelerate the cascading releasing process as follows. After an honest miner publishes a block, every selfish miner publishes all their private chain. And in this case, the miner with the longest private chain will get confirmed, but he/she won't have any blocks left private. Moreover, to simplify possible forking, under the situation that there are multiple longest chains, we assume equal network condition for each miner. Then, each of the branches is selected to be the main chain with equal probability.

Simplified Modeling

The mining process can be viewed as repetitive and identical sub-process as follows. Each starts with one block published an honest miner, and then the selfish miner with longest chain wins. If there are multiple maximum, each wins with probability $\frac{1}{\#(maximums)}$.

Simplification

- Why does this simplification make sense?
- Use Monte Carlo method to simulate the process for a series of millions of blocks, and repeat the process for hundreds of times with different set of mining power distribution, we arrive at the conclusion that the modification will affect each miners' profit only by an insignificant percentage (not exceeding 1/1000), which can be neglected.

Theoretical Results

- From the simplification above, we use some complicated mathematical derivation to show the impact on the system when multiple miners become selfish.
- We analyze the situation where there are n miners with equal hash rate in the system, $(n-1)$ of them are selfish and one of them is honest. (Remark: If all of them are selfish, then no one will publish a block and the system will crash.)
- Then, in each round started with a block mined by the honest miner, the expected number of total blocks generated is

$$\sum_{i=0}^{\infty}(1-\frac{1}{n})^i * \frac{1}{n} * (i+1) = n$$

Impact on the System

- Then, from some mathematical knowledge, we know that, for a sequence of length n, and each element has independent and identical probability to be one of n candidates, then the maximum number of occurrences is in the scale of $O(\log n / \log \log n)$. [Reference: M.Raab: Balls into Bins: A Simple and Tight Analysis]
- As a result, we can use the scaling method (i.e. amplification and minimization), where if the number of block generated doesn't exceed n, we regard it as n, and if the number of block generated if kn where $k > 1$, we can conjecture that the maximum occurrence doesn't exceed $O(k \log n / \log \log n)$ since it's the sum of maximum occurrences of each segment. Thus, the number of confirmed blocks in each round is in the scale of

$$\sum_{i=0}^{n-1}(1-\frac{1}{n})^i * \frac{1}{n} * O(\frac{\log n}{\log \log n}) + \sum_{i=n}^{\infty}(1-\frac{1}{n})^i * \frac{1}{n} * O(\frac{i \log n}{n \log \log n}) = O(\frac{\log n}{\log \log n})$$

Impact on the System

- In conclusion, in each round, n blocks are generated in expectation, but only $O(\frac{\log n}{\log\log n})$ of them are confirmed in expectation, which indicates that, when the majority of the system becomes selfish, it's a total disaster to the whole blockchain, where the effective hash power will be decreased to $O(\frac{\log n}{n\log\log n})$ portion of total power.
- Our results indicate that, it's dangerous if miners become selfish. However, for rational miners, whether it's worth perform selfish mining isn't solved yet, so we move on to it.

Expected Gain for Miners

- For selfish miners, from the conclusion before, each time, they have about $\frac{1}{n}$ possibility to have their chain confirmed, and thus their expected confirmed block in each round is in the scale of
$$\mathbb{E}[\#(\text{blocks for selfish})] = O(\frac{\log n}{n \log \log n})$$
- For honest miners, by iterating on the number of miners who mine one block exactly (denoted by i), we can compute their expected confirmed block in each round as follows (Reference: https://math.stackexchange.com/questions/4061018)

$$\mathbb{E}[\#(\text{blocks for honest})] = \sum_{i=1}^{n} \frac{1}{i} \binom{n-1}{i-1} (i-1)! (\frac{1}{n})^{i} = \sum_{k=1}^{n} \frac{(n-1)!}{n^{k}(n-k)!} = O(\frac{\log n}{n})$$

Expected Gain for Miners

- $$\mathbb{E}[\#(\text{confirmed blocks for selfish miners per round})] = O(\frac{\log n}{n \log \log n})$$
- $$\mathbb{E}[\#(\text{confirmed blocks for honest miners per round})] = O(\frac{\log n}{n})$$
- From the comparison above, we can find out that, when n gets sufficiently large, selfish mining isn't a rational choice for self-interest-driven miners, and Bitcoin system is secure from such attacks when hash power gets well decentralized.

Simulation Results

- Then we focus on how the situation will be if the number of miners aren't sufficient. Not able to find a good modeling, the following results are mostly derived from simulation. And we find some equilibrium states.

Nash Equilibrium of the System

Modeling

The system has n ($n \geq 3$) miners with equal hash rate. They're all self-interest-driven and have equal network conditions. Each miner only has two possible strategies, one is honest mining, and the other is selfish mining.

- By simulation, we've found out that, the Nash Equilibrium is that:
  - If $n \geq 4$, all miners are honest.
  - If $n \leq 15$, $(n-1)$ miners become selfish and 1 miner remains honest.
- In these cases, no miners can improve their gain by unilateral deviation.
- The results are based on millions of blocks each experiment and a repetition of hundreds of experiments, and the data is stable between experiments, showing the reliability of the results.

Dynamic Equilibrium with Distinct Hash Power

Assumption

Usually, all miners are honest in the beginning. Suppose they don't corrupt or communicate, a series of deviation to selfish mining should begin with at least one self-interest-driven rational miner, and then other rational miners will possibly change their strategy according to the current situation, leading to a dynamic and sequential deviation in strategy.

- By simulation, we've found out that, under such assumption, there're at most 4 miners mining selfishly in the Bitcoin system, where the threshold for hash power are $26.5\%, 22.65\%, 20.00\%, 19.50\%$ respectively, then the system is also at a Nash Equilibrium.

Some Other Attempts

- The previous results are based on simulation, but we've found it hard to create a reasonable modeling to explain them. Also, the simulation results are hard to be generalized to distinct hash power for each miners. During the process to find a theoretical modeling and explanation, we've made these attempts.

Some Other Attempts

- Mathematical Derivation: However, if users have different hash power, with the same modeling as before, it's quite difficult to directly compute their expected gain.
- Convert Discrete Case into Continuous Case: This idea is borrowed from another paper (M.Van Dijk, et.al. **FLIPIT: The Game of "Stealthy Takeover"**), where we measure each miner's profit on a continuous timeline, and selfish mining can be regarded as taking a part of timeline to be one's own. However, we find it hard to design a function of utility with the variation of time that is consistent with our simulation results.
- I've also noticed that MDP Analysis is a fashion in analyzing selfish mining and designing protocols, which is seen at several well-known papers (Roi Bar Zur et.al. **Efficient MDP Analysis for Selfish-Mining in Blockchains**), and tried to apply similar ideas into the analysis.

Termination

- With all these attempts ending in vain and difficulty in finding a suitable approach for theoretical analysis, we terminate this project.
- Although it's terminated, I think the simulation results and the theoretical results for large n is interesting and is worth exploring.
- Don't hesitate to contact me through marco.cheng712@gmail.com if you have some good ideas about this.

The End.
Thanks for your Attention!