Analyzing Selfish Mining in Proof of Space-based Blockchain Protocols

Amirali Ebrahim-zadeh

Institute of Science and Technology Austria

October 11, 2022

Roadmap

Introduction

Mining, Electricity Consumption, and Climate Change

Alternatives to Proof of Work

- Mining in proof of work-based blockchain protocols wastes huge amount of electricity, due to CPU power required for solving cryptographic puzzles.
- Some cryptocurrencies use other resources for block generation. Alternative resources include:
  - Stake in proof of stake
  - Hard drive space in proof of space (e.g. Chia)

Our Contribution

- Due to the value of cryptocurrencies, it is important to guarantee their security.
- Selfish mining: A possible attack, threatening the security of Bitcoin.
- How vulnerable are PoSpace/PoStake-based protocols against selfish mining?
- What we did:
  - Designing a selfish mining-style attack against Chia
  - Modeling the attack as an infinite-state Markov chain
  - Analysis and verification of the model

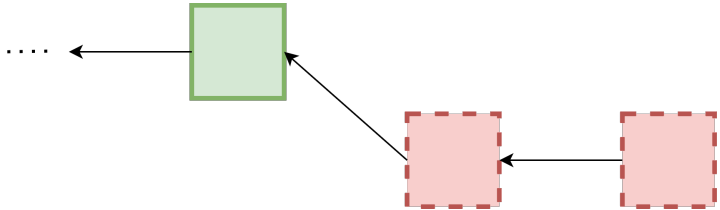
Selfish Mining Attacks

What is Selfish Mining?

- An adversary keeps its discovered blocks in private.
- This will waste the honest miner's hashing power to mine blocks that will never end up in the main chain.
- At least 25% of the network's hashing power required for a successful attack in Bitcoin.

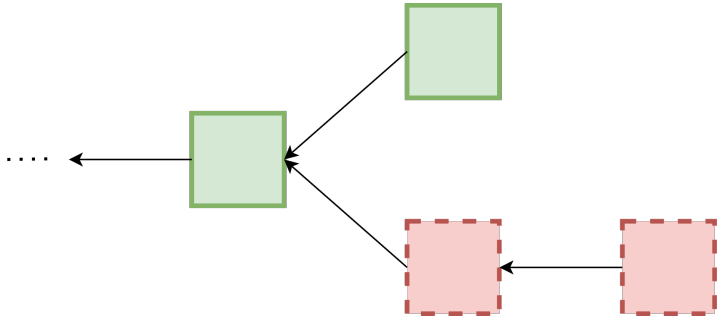
A Simple Example

Honest blocks in green, adversarial blocks in red, and private blocks are dashed.



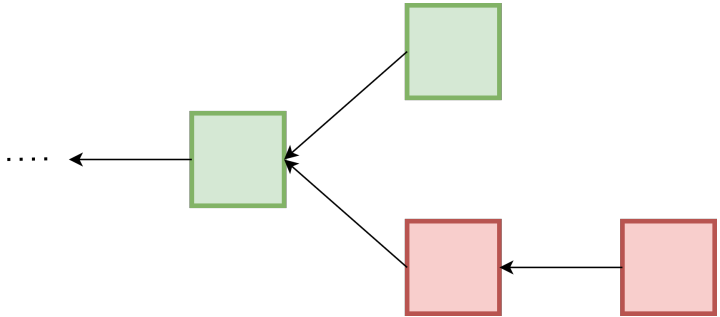
A Simple Example

Honest blocks in green, adversarial blocks in red, and private blocks are dashed.



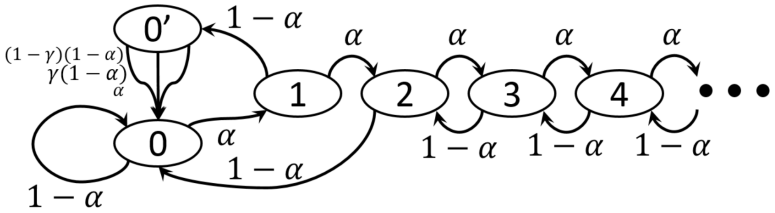
A Simple Example

Honest blocks in green, adversarial blocks in red, and private blocks are dashed.



Modeling the Attack as a Markov Chain

- The fraction of adversarial resource denoted by α
- Each state representing the lead of the adversary i.e. the number of blocks in the private chain
- Full analysis found in "Majority is not Enough: Bitcoin Mining is Vulnerable"

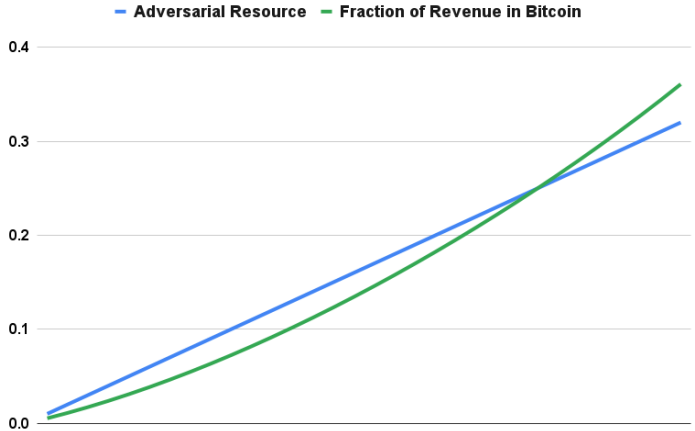


Steady State Reward

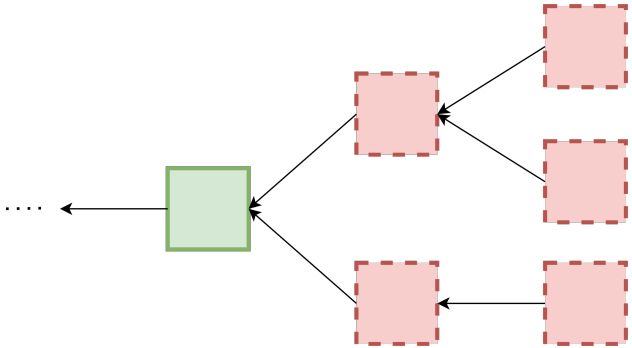
$$R_{adv} = \frac{r_{adv}}{r_{adv} + r_{honest}} = \frac{\alpha(1-\alpha)^2(4\alpha + \frac{1}{2}(1-2\alpha)) - \alpha^3}{1 - \alpha(1 + (2-\alpha)\alpha)}$$

Analysis

For $\alpha > 0.25$ the attack will be profitable.



Private Tree Instead of Private Chain



Modeling

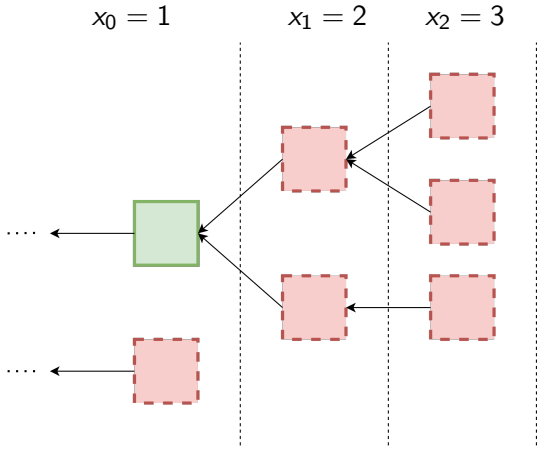
Need for a New Model

- The model for Bitcoin only represents the lead of the adversarial chain.
- A model for selfish mining in PoSpace must capture the state of the private tree. More than one parameter is needed.

The Model for PoSpace

- Like in Bitcoin, we model the attack as an infinite state Marcov chain.
- States: vectors like $x = [x_0, ..., x_d]$ where x_i is the number of private blocks at depth i, and d is the total depth of the private tree.
- Transitions: homographic functions of α (fraction of resource controlled by adversary)
- Topology of the tree does not matter.

Example



The corresponding state is $x = [1, 2, 3]$.

Bounding the Infinite State Markov Chain

- There are no bounds on d, the depth and w, the width of the tree or maximum number of blocks at each depth.
- We set $d = 6$ and $w = 6$ to make analysis feasible.

$$|S| = (w+1)^{(d+1)} \approx 8.2 \times 10^5$$

- The precision of the analysis will be good, due to the improbability of a lead more than 6 blocks.

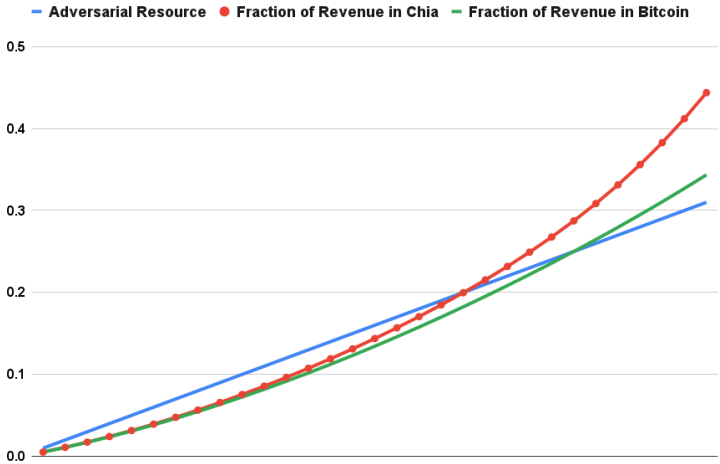
Analysis

Model Chacker

- We used PRISM, a probabilistic model checker.
- We verified the steady state reward properties for $\alpha = 0.01, 0.02, ..., 0.30$

Security Threshold

The security threshold in PoSpace is 0.2, less than 0.25 in Bitcoin.



Conclusion

The adversary requires at least 20 percent of the total network's space to perform a successful selfish mining attack. The threshold can be slightly less if more optimal strategies are found, and increased if defense mechanisms like correlated randomness are adopted.

Future Steps

What's Next?

- Design and Analysis of more optimal attacks
- Modeling defense mechanisms like c-correlated randomness

Summery

What We Did

- Generalizing selfish mining; adapting to PoSpace.
- Modeling the attack as an infinite state Markov chain.
- Bounding and analyzing it with a model checker. Computing the security threshold.

Previous Directions

- Finding new chain selection rules to reduce the adversary's revenue in Bitcoin.
- Countering double dipping attacks in PoSpace.