Majority Is Not Enough: Bitcoin Mining Is Vulnerable

Financial Technologies and Applications (T-714-FINT)

Giorgio Saldana

Reykjavík University

6 December 2024

Introduction

Bitcoin: A Decentralized Cryptocurrency

- Peer-to-peer digital currency.
- Transactions recorded on a blockchain.
- Miners solve cryptographic puzzles to validate transactions.

Key Feature: Decentralization

- No single entity controls the blockchain.
- Assumes miners act honestly.

Bitcoin Mining Background

How Mining Works:

- Miners compete to solve cryptographic puzzles.
- Winner appends a new block to the blockchain.
- Longest chain is adopted as the valid chain.

Rewards:

- Block reward + transaction fees.
- Mining power (α) determines the probability of solving the puzzle.

Problem Statement

Assumption: Honest Mining is Incentive-Compatible

- Miners are rewarded proportionally to their mining power.
- Mining pools reduce income variance.

Reality: Vulnerability to Collusion

- Selfish mining strategy allows colluding miners to earn disproportionate rewards.
- Threatens Bitcoin's decentralization.

Selfish Mining Strategy

Key Idea:

- Keep discovered blocks private.
- Force honest miners to waste resources on the public chain.

Steps:

(1) Mine privately and maintain a hidden chain.

(2) Publish private chain strategically to invalidate honest miners' work.

(3) Gain a higher share of rewards.

Finite State Model

States:

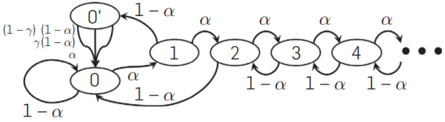
- 0: No private lead.
- 1: Selfish miners have a 1-block lead.
- k: Selfish miners have a k-block lead.

Transitions:

- Selfish miners mine a block: Move to $k+1$.
- Honest miners mine a block: Publish private chain.

Tie State ($0'$):

- Honest and selfish chains have equal length.
- Resolved by honest miner behavior (γ).



Revenue Events for Selfish and Honest Miners

Key Revenue Events:

- **(a):** Pool appends to its private branch, increasing its lead. Revenue counted later.
- **(b):** Pool has lead 2, publishes chain, earns revenue of 2.
- **(c):** Others find a block at head, lead drops to 1. Pool and others earn 1.
- **(d):** Others find a block after head in a tie. Others earn 2.
- **(e):** No private branch; others find a block. Others earn 1.
- **(f):** Lead is 1; others find a block. Pool publishes, creating a tie.
- **(g):** Lead is 2; others find a block. Pool publishes, earns 2.
- **(h):** Lead > 2; others find a block. Pool reveals i-th block, earns 1.

Mathematical Formulation

Revenue Contributions:

$$r_{\text{others}} = \underbrace{p_{0'} \cdot \gamma(1-\alpha) \cdot 1}_{\text{Case (c)}} + \underbrace{p_{0'} \cdot (1-\gamma)(1-\alpha) \cdot 2}_{\text{Case (d)}} + \underbrace{p_0 \cdot (1-\alpha) \cdot 1}_{\text{Case (e)}}$$

$$r_{\text{pool}} = \underbrace{p_{0'} \cdot \alpha \cdot 2}_{\text{Case (b)}} + \underbrace{p_{0'} \cdot \gamma(1-\alpha) \cdot 1}_{\text{Case (c)}} + \underbrace{p_2 \cdot (1-\alpha) \cdot 2}_{\text{Case (g)}} + \underbrace{P[i>2](1-\alpha) \cdot 1}_{\text{Case (h)}}$$

Revenue Ratio for the Selfish Pool:

$$R_{\text{pool}} = \frac{r_{\text{pool}}}{r_{\text{pool}} + r_{\text{others}}} = \frac{\alpha(1-\alpha)^2(4\alpha + \gamma(1-2\alpha) - \alpha^3)}{1 - \alpha(1 + (2-\alpha)\alpha)}$$

Threshold for Profitability:

$$\alpha_{\text{threshold}} = \frac{1-\gamma}{3-2\gamma}$$

Example: If $\gamma = 0.5$, then $\alpha_{\text{threshold}} = 0.25$.

Revenue Analysis

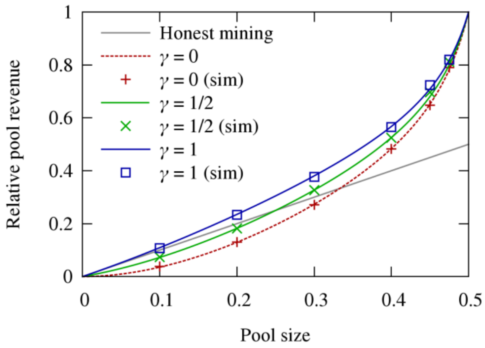
Key Observations:

- Selfish mining is profitable if $R_{\text{pool}} > \alpha_{\text{threshold}}$.
- Threshold decreases as γ increases.
- Superlinear growth: Larger selfish pools attract more miners.

Simulation Results:

- Confirm theoretical predictions.
- Revenue increases with pool size once above the threshold.

Revenue Dynamics



Key Insights:

- **Honest Mining (Gray Line):** Revenue scales linearly with mining power ($R = \alpha$).
- **Selfish Mining (Colored Curves):**
  - $\gamma = 0$: Honest miners resist selfish miners; least advantage.
  - $\gamma = 0.5$: Honest miners split evenly between chains; moderate advantage.
  - $\gamma = 1$: Honest miners fully support selfish chain; maximum selfish miner revenue.
- **Superlinear Growth:** Once $\alpha > \alpha_{\text{threshold}}$, selfish mining becomes disproportionately profitable.
- Simulation results (points) align with theoretical predictions (curves).

Threshold and Pool Growth

Behavior Above Threshold:

- Selfish pool earns disproportionate rewards.
- Rational miners are incentivized to join selfish pool.

Centralization Risk:

- Pool grows unopposed, potentially reaching 51
- Decentralization collapses.

Proposed Solutions

Protocol Modification:

- **Randomized Fork Resolution:** Miners should randomly choose which chain to mine on during ties, reducing the selfish pool's ability to exploit forks.
- **Backward-Compatible Mechanism:** Modifications to the protocol ensure that pools smaller than 1/4 of the total mining power cannot profitably engage in selfish mining.

Impact of the Solution:

- Increases $\alpha_{\text{threshold}}$ to 25% for profitability when the solution is adopted.
- Strengthens Bitcoin's resilience but does not eliminate the threat entirely.

Conclusion

- Selfish mining proves that Bitcoin's mining protocol is not incentive-compatible.
- Without changes, selfish pools as small as 1/4 ($\alpha = 0.25$) of mining power can profit.
- At least 2/3 of the network must remain honest to maintain decentralization and thwart selfish mining. A simple majority (51
- The solution makes attacks harder for smaller pools but does not completely eliminate risks to decentralization.