Title:

Quantifying the Impact of MEV on blockchain consensus security

Team:

Liyi Zhou, Kaihua Qin, Arthur Gervais

Flashbots contact

:

Created:

2020-12-10

Status:

Stagnant

Github:

mev-research/FRP-9.md at main · flashbots/mev-research · GitHub

Quantifying the Impact of MEV on blockchain consensus security

Multiple works have expressed the qualitative intuition that MEV deteriorates (PoW) blockchain consensus security. Yet, we're not aware of any quantitative results supporting this hypothesis. The literature proposes various methods on quantifying (PoW) blockchain security. One common insight is that the stale block rate aggravates the risks of double spending and selfish mining. That means, the more forks we can observe on-chain, the easier game becomes for an adversary to defraud other blockchain participants. If MEV encourages miners to fork the blockchain, MEV would directly deteriorate the blockchain's consensus security. In this FRP we aim to quantitatively reason about the impact of MEV on blockchain security.

Background and Problem Statement

In this FRP, we would like to find the minimum MEV value, at which an MEV-aware miner will start to fork the blockchain to claim MEV. If this threshold is very low (e.g., < 10 times the block reward), then MEV clearly is a danger to the chain. Further, we want to extend the study to a multiplayer game, where multiple MEV-aware miners would engage to compete over an MEV opportunity. We then aim to quantify the average and maximum fork length that we can expect to observe.

By parameterizing a blockchain through its stale block rate, we can capture any PoW blockchain reparametrization (e.g., covering Bitcoin, Ethereum and others). While the results are expected to primarily apply to PoW based blockchains, we would like to investigate to what degree our model would also apply to PoS.

Plan and Deliverables

- Within this work, we aim to provide a model that allows us to identify the optimal mining strategies to exploit MEV given one MEV-aware miner. Given the optimal mining strategies we can then determine the minimum MEV amount, at which a rational MEV-miner would attempt to fork the blockchain. Our results are aimed to be applicable to any PoW blockchain following the longest chain rule.
- We further plan to design a simulation for a multi-miner game as in to understand how multiple MEV-extracting miners would behave when competing. We want to quantify the resulting average and maximum fork lengths under 1,2 or 3 competing miners. We hope that our results would hence quantitatively inform us whether more MEV-miner competition aggravates the blockchain security.
- We plan to understand to what degree our results apply to PoS blockchains.

References

Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges

Liquidations: DeFi on a Knife-edge

On the Security and Performance of Proof of Work Blockchains

Optimal Bidding Strategy for Maker Auctions

Understanding Compound Liquidators - ZenGo