Title:

Mempool Privacy

Team:

HashCloak

Created:

2021-02-24

Status:

Active

Github:

mev-research/FRP-10.md at main · flashbots/mev-research · GitHub

A feature that is missing from MEV-Geth is complete privacy. That is, the ability to keep incoming transactions in the mempool private. As a result, certain kinds of censorship and ordering attacks are still possible despite MEV-Geth's ability to provide pre-trade and failed trade privacy.

The goal of this FRP is to survey privacy solutions that can be used to provide MEV-Geth with mempool privacy and attempt to start formalizing the problem of mempool privacy for L1 and L2 blockchain constructions. Further, we will initially focus on the use of cryptographic primitives for providing mempool privacy. We suspect that for certain L2 constructions such as optimistic and ZK rollups, that there aren't many changes to the mechanics of how the mempool works with respect to privacy but with others such as state channels, we may need to investigate further these differences.

Plan and Deliverables

- Define a set of properties of a desirable mempool privacy solution
- Identify a suitable (or set of suitable) threat models for a mempool privacy solution
- Both for L1 and L2
- Both for L1 and L2
- Identify practical implementation considerations and tradeoffs for relevant mempool privacy solutions
- Focus on currently deployed blockchains
- Focus on currently deployed blockchains
- Inform future blockchain network designs around mempool privacy

Resource List

- MEV Roast: Privacy
- Thwarting Front-Running with Threshold Decryption and other Tendermint Shenanigans
- Multi-Party Timed Commitments
- Tesseract: Real-Time Cryptocurrency Exchange Using Trusted Hardware