Title:

Cryptographic primitives for complete privacy

Team:

JBStearn

Flashbots contact

: @fiiiu

Created:

2021-12-16

Status:

Completed

Github:

mev-research/FRP-18.md at main · flashbots/mev-research · GitHub

Cryptographic primitives for complete privacy

Background and Problem Statement

Flashbots' roadmap sets complete privacy as a core design goal. This means that transactions in the mempool are private until they have been mined on-chain. Complete privacy ensures that no privileged actors (e.g. miners/block proposers) are able to extract MEV through ordering or censorship attacks.

In this FRP, we will survey the current cryptographic approaches to mempool privacy, including verifiable delay functions, threshold encryption, and multi-party timed commitments. We consider the advantages and disadvantages of these methods in terms of defined properties of a complete privacy solution, such as UX, scalability, etc. We assess the security of these methods with respect to a range of threat models. This section of the FRP will consist of a review of the mathematics underlying the respective cryptographic primitives, followed by an analysis of possible application of these methods to Flashbots Auction.

Further, we will investigate zero-knowledge proof approaches as a possible solution to obtaining mempool privacy for Layer 1 constructions and mitigating negative externalities related to MEV extraction.

Plan and Deliverables

We will produce a paper and accompanying blog post(s) outlining research in the following areas:

- Determine required properties & acceptable tradeoffs for a complete privacy solution.
- Literature review of mathematics of cryptographic primitives:
- Verifiable Delay Functions (VDFs)
- Multi-party Timed Commitments (MPTC)
- Threshold Encryption
- ZK approaches:
- Bulletproofs
- SNARKS
- STARKS
- Bulletproofs
- SNARKS
- STARKS

- Verifiable Delay Functions (VDFs)
- Multi-party Timed Commitments (MPTC)
- Threshold Encryption
- ZK approaches:
- Bulletproofs
- SNARKS
- STARKS
- Bulletproofs
- SNARKS
- STARKS
- Outline threat models/implementation issues & tradeoffs for each approach in the context of Flashbots Auction.
- Investigate ZK approaches to L1 & Flashbots Auction mempool complete privacy.

Resource List

- Verifiable Delay Functions
- Threshold Broadcast Encryption
- Multi-Party Timed Commitments
- Submarine Sends
- Dark Pools
- ZK-SNARKS
- ZK-STARKS