Title:

Cryptoeconomic design

Team:

Philip Daian, Alejo Salles

Created:

2021-06-04

Status:

Completed

Github:

mev-research/FRP-14.md at main · flashbots/mev-research · GitHub

Cryptoeconomic design

Background and Problem Statement

While Flashbots is exploring an SGX-based solution to provide complete pre-trade privacy as outlined inthis post, we would like to explore in parallel if there are cryptoeconomic mechanisms that can reinforce, or substitute the relatively expensive and proprietary solution that is SGX, to achieve the same desirable result: namely a fully private way to submit txs to block proposers without having to reveal their content to them so they cannot tamper with it/act adversarially on it.

The aim of this research is to collect thoughts on the topic, write up a short strawman spec and start building more thinking, especially how it relates to eth2 and mev-sgx.

Plan and Deliverables

- strawman proposal of a cryptoeconomic mechanism to provide flashbots functionalities
- include all relevant tradeoffs
- include all relevant tradeoffs
- evaluate merging design with technical specs to reinforce each other (eg. design + sgx)
- think of how eth2 fits in the picture and if there are any mechanisms we can piggy back on
- opt-in slashing conditions?
- any desired protocol changes? if so, draft EIP?
- opt-in slashing conditions?
- any desired protocol changes? if so, draft EIP?

References

- Cryptoeconomic relayer bonding proposal
- Cryptoeconomic design whiteboard sesh recording
- Proposer/block builder separation-friendly fee market designs
- ArcherDAO Private Bundler proposal
- DoS micro-fee and reputation proposals

Output