Title:

Flashbots on Alternative Chain Architectures

Team:

Sikka

Flashbots contact

:

Created:

2020-12-13

Status:

Stagnant

Github:

mev-research/FRP-8.md at main · flashbots/mev-research · GitHub

Flashbots on Alternative Chain Architectures

Background and Problem Statement

The Layer 1 MEV Auction design presented in Paper 1 (aka Flashbots

) is particularly architected for use in Proof of Work Nakamoto consensus based blockchains (more particularly Ethereum). However, as alternative blockchain architectures become more and more prevalent due to rise of “third gen blockchains” (including Eth 2.0, Cosmos, Avalanche, Solana, etc), it is of interest to understand what chain architectures Flashbots

can be easily ported to. For example, can Flashbots

be used on Ethereum as it shifts to Eth 2.0? How about Tendermint BFT-based chains? How about leaderless consensus protocols like Avalanche? Furthermore, are there any differences in the impact of high REV on these different chains vs Ethereum 1.0?

By understanding what chains Flashbots

(and other Layer 1 MEV Auction architectures) can be used to efficiently extract MEV, as well as the properties these chains share, we can better understand how to mitigate those properties in novel architectures to help minimize MEV in next-generation blockchains.

Plan and Deliverables

- Identify what types of MEV-extracting “actions” Flashbots

helps enable

- Describe properties required of a blockchain architecture for above MEV-extracting “actions” to be executable
- Describe properties required of a blockchain architecture to allow Flashbots

’s Layer 1 MEV Auction architecture to function

- Analyze alternative consensus systems of interest (with no state machine changes) to see which of the above properties they satisfy to determine if the Flashbots architecture would be compatible. Particularly:
- Nakamoto-style Proof of Stake (Eth 2.0 Casper)
- Classical BFT (Tendermint/Cosmos)
- Leaderless Consensus (Avalanche) (MAYBE)
- Nakamoto-style Proof of Stake (Eth 2.0 Casper)
- Classical BFT (Tendermint/Cosmos)

- Leaderless Consensus (Avalanche) (MAYBE)
- Analyze the above consensus protocols to see what the impacts of high extracted MEV is and how it differs from Nakamoto Proof of Work (paricularly with respect to consensus instability).
- Describe changes that could be made to a blockchain architecture (other than consensus protocol) to prevent it from meeting properties required for MEV extraction by the Flashbots architecture. Consider changes in:
- Tx readability in the mempool
- Ability for proposer to single-handedly determine inclusion and order of txs in a block
- Tx readability in the mempool
- Ability for proposer to single-handedly determine inclusion and order of txs in a block
- Describe an example construction for an new blockchain architecture in which Flashbots

would not be compatible

References

- Thwarting Front-Running with Threshold Decryption and other Tendermint Shenanigans