Title:

MEV in eth2 - inequality & attack vectors analysis

Team:

Alejo Salles, Barnabé Monnot, Caspar Schwarz-Schilling

Flashbots contact:

@fiiiu

Created:

2021-06-04

Status:

Completed

Github:

mev-research/FRP-15.md at main · flashbots/mev-research · GitHub

MEV in eth2 - inequality & attack vectors analysis

Background and Problem Statement

In the article MEV in eth2 - an early exploration several open questions are raised, some of which we would like to investigate further within the scope of this research proposal:

1. To what extent does Maximal Extractable Value (MEV) in eth2 amplify its inherent rich-get-richer dynamics?

- The protocol provides rewards for validators, validation duties and transaction fees. Additionally, revenue may be received from MEV operations. Finally, all rewards received may be distributed according to some revenue-sharing scheme of the pool/exchange stakers are a part of. We intend to make precise how these dynamics inter-operate.
- Consider the heterogeneity of validators in eth2: solo stakers vs. pooled staking (e.g. Kraken, Lido, etc.). What effect does a varying capability of MEV-extraction have on the equality of the system?

2. How does knowing the block proposers in advance change MEV extraction dynamics?

- Knowing the block proposer ahead of timechanges dynamics, but how does it differ if you have a one-epoch lookup for block proposers (see here for more context)?
- Are consensus attacks (e.g., time bandits/reorgs) due to new MEV extraction dynamics more likely?

Proposed Approach

We are interested in a dynamical systems approach to the problem. A staker with some amount of capital has multiple choices to participate in the staking game: solo staking or pooled staking. Each comes with its own threats and opportunities.

Solo staking

Pooled staking

Opportunities

Full reward, no staking fee

Low capital requirements, possibly offset by staking derivatives; lower reward variance

Threats

Need 32 ETH + infra to stake

Anticorrelation penalties of the protocol increase risk of pooling; staking fee

Over time, we study the growth dynamics of staker types by applying methods from evolutionary game theory. Stakers have their own payoff function and risk preferences. The growth of any particular entity may be limited by the exposure to anticorrelation penalties/limited availability of insurance, deterring risk-averse agents.

Additionally, the protocol introduces reward variance due to the randomness of the block proposer. This variance is possibly compounded by the availability and capability of MEV extraction, in particular for large entities who may be able to realise economies of scale due to multi-block extraction techniques.

Plan

Re 1. To what extent does Maximal Extractable Value (MEV) in eth2 amplify its inherent rich-get-richer dynamics?

- Specify a minimum viable model using the EGT framework
- Heterogeneous validator landscape (staking pools vs. individuals)
- Different scenarios: Perfectly democratized MEV extraction vs. economies of scale vs. (hypothetically) no MEV at all
- Heterogeneous validator landscape (staking pools vs. individuals)
- Different scenarios: Perfectly democratized MEV extraction vs. economies of scale vs. (hypothetically) no MEV at all
- Implement minimum viable model
- Iteratively increase complexity of model until analysis is satisfied

Re 2. How does knowing the block proposers in advance change MEV extraction dynamics?

- Gain a deeper understanding of the RANDAO Game
- Confirm that block proposer one-epoch lookup only holds, if effective balances do not change across epochs.
- Establish to what extent an attacker may manipulate the RANDAO game and if this could be used advantageously to better extract MEV
- Confirm that block proposer one-epoch lookup only holds, if effective balances do not change across epochs.
- Establish to what extent an attacker may manipulate the RANDAO game and if this could be used advantageously to better extract MEV
- Analyse block squashing attack
- Assess potential multi-block strategies
- Study consensus security/finality threats that may arise from MEV (analogs to time-bandit attacks)

Expected Deliverables

Re 1. To what extent does Maximal Extractable Value (MEV) in eth2 amplify its inherent rich-get-richer dynamics?

- Publish a notebook with simulations and visualizations of said centralizing dynamics

Re 2. How does knowing the block proposers in advance change MEV extraction dynamics?

- Publish a note discussing and analysing said topics

References

- What Happens After Finality in ETH2? - HackMD
- Uncle risk/MEV miner fee calculation - HackMD
- naiveurn
- RNG exploitability analysis assuming pure RANDAO-based main chain - Sharding - Ethereum Research
- https://twitter.com/tkstanczak/status/1396178139445927937?s=20
- https://twitter.com/samuelshadrach4/status/1401965712223064064?s=21

- https://twitter.com/kristofgazso/status/1396214165115744267

Output

While some of the work here is still in progress (like getting more numbers on the impact of MEV rewards on centralization), FRP-15 is now being closed in favor of new efforts and collaborations.

Below are some of the works that were influenced by FRP-15:

- MEV-boost: Merge ready Flashbots Architecture MEV-Boost: Merge ready Flashbots Architecture - The Merge - Ethereum Research
- Three Attacks on Proof-of-Stake Ethereum [2110.10086] Three Attacks on Proof-of-Stake Ethereum
- RANDAO manipulation exploration notebook by @casparschwa and @barnabemonnot RANDAO manipulations
- Ethereum economic model extended to have per validator reward accounting, allowing to specify a custom MEV reward process (useful to e.g., look at validator balance distributions in various scenarios): https://barnabemonnot/ethereum-economic-model@b3a3e8d