Zero MEV

2nd of July, 2021
v5. 4th of July, 2021
Marcos Mayorga

Introduction.

In the blockchain space an important problem related to MEV (Miner Extractable Value) is now mainstream.
The ‘bug’ was always there, it is now shallow.
The system baptised as **Plebble** was on the whiteboard in early 2017, searching for a more egalitarian system, resulting on a Zero-MEV system free from the problem exposed by systems where miners/validators can obtain extra profits at the detriment of the system users.

The problem.

- It is a problem affectintg systems based on Nakamoto consensus: PoW, PoS, Po*
- It consists on the ability a miner/validator has of reordering transactions to maximize their profit.
- Originally it was fine design allowing miners to select transactions with higher fees.
- Since DEFI is based on trading, arbitrage conditions, a miner can be improved to watch the mempool looking for transactions that take advantage of any profitable market condition, removing these transactions and adding their own hence collecting (stealing) their profit. (ref. flashbots)
- This is an unacceptable unfair condition for the user.
- **It cannot be easily fixed** since the bug is deep into the core design of nearly all blockchain systems.

The problem not only applies to Ethereum (host of major DEFI projects where effects are more apparent and severe) MEV is also happening in Bitcoin, since miners choose the order that max their profits, causing low fee tx to be delayed. This is commonly sold as a feature but is rather an imperfection.

Plebble. A Zero MEV system.

Plebble is based in novel design consensus algorithm with aims on:

- Maximize distribution of nodes/validators.
- Zero economic bias. Poor and rich participants all have the same profit for the same actions.

Nakamoto consensus (competitive) highlights:

- Foundation of all major mainstream blockchain systems.
- Every validator/miner calculate a different block based on their freedom in crafting blocks - origin of the MEV problem.
- One miner/validator is choosen on every consensus cycle to decide the block.

Plebble consensus (cooperative) highlights:

- Every validator/miner calculating the same block, all of them win the block.
- Requires transaction ordering included in consensus from its root design.
- Any manipulation from the miner/validator and they won't succeed with their block.
- The Key or magic sauce, Plebble’s genuine innovation:

- Timestamping transactions at origin. User decide execution time and is included in the signature.
- Users do not decide fees.
- A BFT consensus algorithm where all honest validators/miners calculate the same block.

More information.

Plebble is Zero MEV by design, and together with further features is arguably the most egalitarian and efficient consensus system available with the lowes entry barrier for participants.
Researchers are looking for solutions to fix mainstream systems, but there is not a clear viable path.
Plebble was developed in stealth mode mostly for avoiding distractions, to prove the system by making it rather than by selling the idea and capture premature atention. We don't sell promising smoke.
The project is now progressively looking for ways to capture genuine attention from researchers, developers and positive thinkers advocating ideas for a better economic and future social systems.
Even though our main milestone (deploy last alpha, starting beta) is nearly completed, documentation has just begun to flourish. Feel free to engage in conversation avoiding insane comparisons with other, more mature, respectable and trustable systems like Bitcoin or Ethereum.

Protocol change. Proposal.

In good faith towards non-plebble systems I would like to suggest to consider **patching Nakamoto-consensus based protocols** in a way that transactions are timestamped at origin (allowing users to set the desired time for execution). That would give miners a straight-forward ordering rule plus adding a new block validation rule requiring transactions be ordered by the new transaction-execution field (which can be expressed with nanosecond precision using an unsigned 64 bit integer).
The improvement would reduce considerably (although not mitigate completely) miner's ability to gamble on the order. They could still remove or frontrun user transactions with their own transactions. The full Zero-MEV solution can be found on Plebble's cooperative consensus.

References.

- MEV summit - 1st of July, 2021
  - Recording https://www.youtube.com/watch?v=s3nACF7uVZw
  - Summit Agenda and Slides https://hackmd.io/ivUzk3piQEG8ALzCGbxlag

- Plebble. Testnet
  https://plebble.net