Background

The MEV Committee is a grants-funded initiative to help the community enforce a social mitigation strategy against malicious block proposers. The committee was assigned to actively monitor, analyze, and report any potential MEV activity, so that the community may respond appropriately to bad actors.

The Committee was recently renewed with a smaller contributor base and slightly revised scope of work. Our initial term pointed to no obvious MEV activity among the active validator set, but rather unintentional performance issues that sometimes resulted in a similar degradation of the trading experience. We now aim to keep the community updated of issues found among validators, whether malicious or performance-related.

August Activity

We have been monitoring discrepancies across block proposers and nodes, following the revamp done by the Rockaway team with the dashboard, leveraging the original Skip API. There were multiple instances of high discrepancy in the past month that required further review.

In summary, a few outlier blocks with relatively high order book discrepancy were detected this past month. Large discrepancy blocks were noticed during periods of high market volatility, including large liquidation events and network activity. Following in-depth reviews, we conclude that no malicious activity occurred during these events.

We also reviewed blocks with smaller amounts of discrepancy, which we found to be caused by abnormally large trade orders. Again, no malicious activity was detected. However, we do suspect issues with order gossiping and network peering across validators may be at fault.

Below, we outline in-depth a few of the cases found as an example of discrepancy data identified and our processes for examining them.

Blocks Analyzed

Additional data and insights can be found in the following repository:GitHub - dydx-jordi-mev-committee/august_report

Block 22033655 – $6k discrepancy

Block 22033672 – $8k discrepancy

Block 22033678 – $5k discrepancy

On Aug 5th 2024, we found a handful of blocks showing high discrepancy, all of which happened in a time of high market volatility. The most notable include the three blocks mentioned above. The blocks appeared relatively near one another, and were proposed by different validators, implying that discrepancies may have been a result of market and network activity rather than any individual issue.

Further analysis shows us that discrepancies originate mostly from orders being matched differently across nodes, which we suspect is a result of high network activity and congestion. Liquidations, which are performed locally by the block proposer, can also trigger discrepancies given higher likelihood of variance in execution. Given the high volume of liquidations occurring throughout these blocks, we attribute them as a likely cause of the discrepancies.

Block 22647118 – ~$1k discrepancy

A trader placed an order to sell 10 BTC at a price of $58,000 for $580,000. The block was proposed with a mid-price of $58,378, implying the order was treated as a market taker order. The proposer matched the order with 26 open maker orders at an average price of $58,354.23. According to our node, the order could have been matched against a different set of 28 open maker orders at an average price of $58,263.16.

We assign differences in matching to the size of the taker order and liquidity available to execute.

Block 22651850 – ~$1k discrepancy

A trader placed two open stop losses, 40 ETH at $2,649.00 for $105,960 and 35 ETH at $2,651.00 for $92,785. The block was proposed with a mid-price of $2,652.80, triggering both stop loss orders. The proposer matched the 75 ETH with 8 maker orders at an average price of $2,639.21. Our node matched the 75 ETH with 27 maker orders at an average price of $2,648.96.

Again, we suspect the differences originate from the size and possible networking issues limiting access to all open orders.

Block 22893647 – ~$1k discrepancy

A trader placed an order to sell 2 BTC at $58,688 for $117,376. The block was proposed with a mid-price of $58,743. The proposer matched the order with 13 maker orders at an average price of $58,264. Our node matched with 12 maker orders

at an average price of $58,733.50.

Analyzing our matches against the proposer, we find that a significant amount of our maker orders were submitted near the block time. We suspect the proposer did not receive these orders in time to process them, potentially a result of poor peering by the validator node.

Conclusion

In August, the MEV Committee continued its monitoring and analysis of block discrepancies among validators to identify potential malicious MEV activity or performance issues. We found several blocks with significant order book discrepancies, particularly during periods of high market volatility. However, after thoroughly reviewing each case, we found no evidence of obvious malicious activity across the validator set.

The discrepancies observed were primarily attributed to factors like large trade orders, network congestion, and possible networking issues that affected the dissemination of order information among nodes.

Overall, while no malicious activities were detected, our findings suggest that there are still areas for improvement in network performance. We will continue to closely monitor these issues and provide updates to the community to ensure the integrity and fairness of the trading environment.