## Background

The MEV committee is a grants-funded initiative to help the community enforce a social mitigation strategy against malicious block proposers. The committee proactively monitors, analyzes, and reports on MEV activity on dYdX v4, so that the community can respond appropriately to malicious actors.

In the previous report, we described our process for monitoring and analyzing possible events of MEV on dYdX v4. In this report, we'll walk through the next step in our process: investigating and responding to positive events identified in our analysis.

## Investigating MEV Events

If we find a block including positive discrepancy data, which was not a result of latency or jitters, the committee will take action to further investigate the possible cause. The same applies for trends forming across cumulative discrepancies, where a proposer's individual blocks may not warrant concern but the sum of all their discrepancies indicate problematic behavior.

As with latency issues, there's still a possibility that the discrepancy is a result of non-malicious behavior. We want to avoid jumping to conclusions and accusations at every sign of MEV. Instead, our goal is to leverage both on-chain and off-chain data points to cross-reference all the possible causes, such that any accusation of MEV is made with confidence.

First, we explore relevant on-chain data beyond an individual event or block to look for possible trends or indications of malicious activity. For example, is the block proposer repeatedly matching orders at a worse price against a single subaccount – implying a strategy to always benefit their own trading account? Or do we see the same cause for discrepancy appear in each block – implying a specific strategy deployed by the proposer (e.g. sandwiching)? Again, Numia's dataset gives us the necessary tools to answer these questions. We use their tables to query validator specific data that could help us identify patterns and behaviors in their blocks.

In parallel, we also try to open a line of communication with the validator directly. This may not always be possible with anonymous validators or teams not wanting to chat, but we find most validators in the active set are open to discussions. Our goal is to work with the team to identify any non-malicious causes for discrepancies, and give them a chance to explain their reasoning for any discrepancies. By exploring their configurations and setups, we can point them to any changes that could resolve the issue. Naturally, discussions are to be taken with a grain of salt since a malicious proposer may hide or distort information to conceal their real intentions – to extract MEV.

Based on the above, we end up with three different outcomes:

1. Non-malicious causes.

The on-chain data shows no obvious trends, and the validator team has identified their issues and/or shared configurations that confirm the cause of discrepancies.

1. MEV activity.

On-chain data shows obvious MEV patterns, and the validator is either uncooperative or incapable of justifying the cause for discrepancies.

1. Inconclusive.

The on-chain data shows no obvious trends, and the validator team is either uncooperative or incapable of justifying the cause for discrepancies.

Ultimately, MEV activity is what we're after. Our primary goal is to stop malicious validators from willfully harming users with extractive strategies. However, we also want to flag non-malicious discrepancies and inconclusive results. Even if unintentionally done, a validator with a high degree of orderbook discrepancy is nonetheless harming the protocol and users with their operations. While we may not recommend direct action for these types of findings, the community should absolutely be aware of validators causing any kind of issues to the trading experience. Delegators and/or the community may still choose to respond for the sake of improving the protocol's overall stability and experience for users.

## Findings

In January, the committee identified one positive case of discrepancy data that merited further investigation.

#### P2P

Background

In early January, P2P started displaying above average levels of cumulative discrepancy data. No single block displayed concerning amounts, but the sum of all their blocks put them above every other validator in total discrepancies. We found no immediate trends or patterns in the blocks produced. The data appeared random in terms of causes for discrepancies. For

example, one block may have missed expected matches for a given market, and the next matched orders for a separate market in a random way. This could imply an issue with their setup instead of malicious behavior.

On January 20th, P2P proposed a block with $1,291 in discrepancy, the highest amount seen by a significant margin. The block included an order executed way below market price, triggering the large discrepancy. Our analysis shows P2P matching a user's stop loss order with maker orders below the current market price, many of which would be considered stale (older orders sitting at a non-competitive price). Mempool data showed a considerable amount of better orders available to execute with, which would have improved the price at which the order was filled.

A separate report on this incident has been detailed at lengthhere. The committee is now exploring methods of resolving these types of user-impacted incidents in the future. We intend to publish a framework that explores recovering funds or making whole users impacted by poor execution.

Following this event, the committee contacted P2P to better understand the cause of their discrepancies. Based on our discussions, we understand that P2P had been experimenting with their node configurations to maximize their validator's uptime. Validators are required to sign all blocks as a confirmation of their validity; uptime represents the number of blocks signed by the validator. A validator not signing enough blocks, or failing to maintain sufficient uptime, will be jailed by the protocol. dYdX v4 has been trickier to manage for some teams given the sub-second block times.

Reviewing their configuration, the team identified an issue with the value used for TTLNumBlocks, a variable that defines the amount of blocks a transaction can exist for in the mempool. By setting this amount to 0, P2P's mempool was not removing older orders from their local mempool, which in turn prevented them from receiving newer orders due to capacity restraints. This setting explained the behavior found in the high discrepancy block – P2P's mempool was clogged with older orders and matched the stop loss against what they viewed as the best available maker orders. Other validators with default configurations may have executed the stop loss using more recent, better maker orders.

With their configuration updated, P2P's numbers improved for a week, but started degrading in the last week of January following the dYdX v3 upgrade. We flagged these issues to P2P again for them to consider further improvements. Since then, P2P has redeployed their validator to fully default configurations, and increased their hardware capacity to improve their overall performance. As of today, P2P's validator is showing an improvement in discrepancy data. Going forward, we're keeping a close eye on P2P's numbers. Large discrepancies come at the expense of the end-user trading experience, which we believe is important to mitigate. We heard from market makers expressing concern over their execution on P2P proposed blocks in the past month.

Assessment

Given our discussions and on-chain analysis, we have no reason to suggest P2P is actively pursuing MEV strategies. The team has been proactively attempting to resolve their issues, and is engaging regularly with the committee. We believe non-malicious problems with their validator is the root cause of discrepancies.

However, these issues should be concerning to the community. Malicious or not, a validator with high discrepancies degrades the trading experience for dYdX users. Matching users against stale maker orders, or failing to maintain consistent execution, is not something we should accept from any validator. The problem is also isolated to a single validator. Other validators have not experienced any issues of this nature in the past month. As such, the community should seriously consider P2P's history of discrepancies when choosing where to delegate.

P2P have recently shown improvements following discussions with the committee. However, these previous issues may suggest that they are not suited to maintain protocol stability and a consistent trading experience for our users. If P2P's performance regresses or begins to show inconsistency again, the committee will recommend more severe measures, such as a formal recommendation to undelegate.

## Future Work

Following our experience with configuration adjustments, we are now writing a guideline for improving validator performance and minimizing the likelihood of discrepancies. The guideline will be published for all validators to reference when assessing their own performance issues. In the meantime, we'll continue to explore on-chain activity, keeping an eye on MEV trends and spikes.