Background

In light of concerns with validator-driven MEV activity on the dYdX Chain, the communityadopted a governance-enforced social slashing model to disincentivize bad actors. Using Skip's contributions to measure potential MEV activity in the form of orderbook discrepancies, the community can identify validators engaging in harmful behavior. The mitigation strategy was designed to retroactively punish malicious validators with both reputational damage and economic consequences, enforced through slashing proposals. The existence of a credible threat to validators, and their delegators, serves as a deterrent to potential malicious intentions.

As part of this strategy, the dYdX Ecosystem Development Program appointed a committee to carry out the role of monitoring activity, analyzing discrepancies, and recommending actions on behalf of the dYdX community. Our goal was to improve the strategy's efficiency through active monitoring, which in turn strengthens the credible threat to bad actors.

The initial six month term for this committee has been completed. In this report, we share an overview of the activities carried out and our findings from this first iteration of the MEV Committee. We also share updates to the MEV mitigation strategy, including changes to our committee and the dashboard.

What we did

The primary role of the committee is to actively monitor the chain for any real-time discrepancies and identify behavioral trends developing among the active validator set. The dYdX Chain averages roughly one block every second, meaning that validators are proposing upwards of 70,000 blocks per day. In theory, any one of those blocks could include malicious MEV activity. That's a lot of blocks to keep an eye on, and it's a lot of data to analyze!

With that in mind, we developed a few additional resources on top of the dashboard to improve our real-time monitoring and analysis capabilities. These included:

1. Running a dedicated full node with mev-telemetry enabled to serve as both a real-time alert system and as a block-by-block data analysis tool.
2. Feeding block data real-time to a dashboard like Datadog or Grafana, we can create rules to trigger an alarm any time a block is proposed with high discrepancies – alerting us to potential MEV activity.
3. Skip's dashboard provides a high level overview of proposer activity, but does not include in-depth data on each block proposed. This data is needed to analyze the contents of the orderbook proposed, including each order match and the source of discrepancies found. By running our own telemetry service, we now have access to all the granular data necessary to analyze suspicious blocks.
4. The DEP also funded Numia to build a custom indexing service for all transactions found in the dYdX Chain mempool. Using this dataset, we can query specific time intervals to identify on-chain activity, and how it might relate to discrepancies found in a block.
5. The Indexer API also provides additional methods of querying user orders, fills, and trading activity across specific subaccounts.

Combining all of these data points together using internal dashboards and custom scripts, we can quickly analyze blocks with the goal of identifying the root cause for any discrepancies. Our primary data point remains Skip's dashboard as the source of truth, given its robust infrastructure and processes, but these extra steps allow for more in-depth analysis and real-time alerting.

Armed with the appropriate tooling, we got to work monitoring blocks!

What we found

The good news: there was no explicit MEV activity found.

However, what we did find is that validators can, and did, impact order execution, at times harming the experience for dYdX traders. Skip's dashboard identified several instances of validators proposing blocks with high discrepancies, deviating from the expected order matching behavior. Below, we share a few of the major events from this first term:

- In January, P2P displayed above average levels of cumulative discrepancy data. No single block displayed concerning amounts, but the sum of all their blocks indicated issues with their order matching process. Our investigation in the issue included analyzing individual blocks and discussing the problem with P2P directly. Ultimately, wefound the root cause to be their node configuration. The node was configured such that their local mempool was not removing older orders, preventing them from receiving newer orders due to capacity restraints. As a result, their local orderbook was stale, matching new market orders with limit orders with stale market prices.

After fixing their configuration, P2P's discrepancy data reduced over time and remained low for the rest of this term.

- In April, we took note of discrepancies appearing among a handful of validators, including Keplr, Validation Cloud,

Ledger by Meria, Informal, and some others. These issues were also flagged to us by market makers, expressing concerns with their orders not executing as expected. Given the fact that multiple validators were at fault, each with different reputations and incentives, we found it hard to suspect malicious intent. Still, we set out to identify the root cause by analyzing trends and looking into validator configurations. We reached out to each team with questions and requests for configuration files.

Ultimately, we found the issue to be a result of protocol changes, specifically soft upgrades including v.4.0.5 and v.4.1.2. Since these upgrades are non-consensus breaking, validators can continue to participate in the block proposals without updating their binary configurations. However, upgrades can impact performance, and not upgrading in a timely manner may have impacted performance relative to other validators.

Once all the validators moved over to v.4.1.2, which also included protocol performance improvements, the issues were largely resolved and market makers reported improvements.

- Throughout the term, we also identified individual one-off events that raised suspicions. For example, in July we noticed consecutive blocks with high discrepancies and severe volatility in price execution. Below is a screenshot of the BTC-USD market at the time, where we see large spikes on both sides of the market.

Analyzing the orders matched, we found the root cause to be a single trading account placing abnormally high market orders. The trader submitted a 50 BTC (~$3M) buy market order and then immediately following execution another 65 BTC (~$4M) sell market order. These orders were large enough to wipe out liquidity, leading to high spreads execution. Based on our findings, this was no fault of any validator, but a result of user activity.

Other such findings were found throughout the term. Oftentimes, this type of activity can result in high discrepancy data. This can happen when the order isn't gossiped across the entire network, leading to some nodes not agreeing with the vastly different orderbook proposed.

[

Screenshot 2024-08-28 at 1.31.54 PM

1304×672 252 KB

](https://europe1.discourse-cdn.com/flex013/uploads/dydx/original/2X/9/9c59c637651f99fed937431700f514f5406f3b4d.png)

Though there were some issues identified, we found no reason to suggest any MEV activity was being conducted by validators.

What we learned

There's a lot more to it than just malicious intent! At launch, our expectations were that discrepancies would happen primarily due to malicious behavior, with maybe the occasional false positive. What we learned is that lots of different factors can influence discrepancy data and order execution, including validator performance, honest configuration problems, protocol upgrades, and user-based errors (e.g. outsized market orders).

Performance Matters

Instead of policing malicious behavior, we found ourselves chasing validators with performance-related issues. The dYdX Chain is a high throughput protocol with at times sub second block speeds and heavy transaction loads. To provide the best experience to users, validators must be performant enough to keep up with the activity. Though not malicious by nature, we do ultimately consider a lack of performance to be unacceptable, given the outcome is similar to users.

Configurations and Upgrades

In other protocols, it's common for validators to run custom node configurations with the goal of optimizing their hardware setups. On dYdX, however, we found that a deviation from the recommended optimal configuration can significantly impact order execution. We published a guideline for validators to follow, including node configurations, hardware requirements, and geographical distribution. We found ourselves chasing after custom configurations more so than the underlying behavior as root causes for discrepancies.

User Errors and Order Gossiping

We learned that not all discrepancies are a fault of the block proposer. At times, users submit presumably erroneous orders that trigger a flurry of activity (including high volatility and unwarranted liquidations). A block proposer executing on the order may display high discrepancies and appear malicious given the unusual execution, when really they're performing as expected.

Similarly, we found some orders fail to gossip in time for an honest block proposer to include them in their block. This is not necessarily a fault of any given validator, more so the network topology (node peering routes) and RPCs used for order submission.

We had initially hoped to publish a framework for standardizing MEV data interpretation, with the goal of implementing a more systematic approach to slashing bad actors. Given the nature of our findings, which includes much more false positives than expected, we don't find it prudent to act on systematic data triggers just yet. The high degree of variance in discrepancy causes could result in unintended consequences to honest participants.

What's next

Following the completion of our initial term, the dYdX Ecosystem Development Program has renewed the Committee for another six month term. This renewal comes with revisions to its size and updates to the dashboard used.

Committee

The MEV Committee now has three core contributors:

- Jordi

Our newcomer to the committee, Jordi is an experienced blockchain data analyst and researcher with in-depth knowledge of validators.

- 0xCLR

An existing committee member, and long time contributor to the dYdX protocol. 0xCLR has tremendous experience in analyzing market activity and data analysis.

- Reverie

An existing committee member, Reverie led the launch of the MEV committee and continues to serve as an advisor to the committee through its existing role as Grantor to the dYdX Ecosystem Development Program.

Why reduce the number of contributors?

Our primary goal going forward is to perform data analysis and share in-depth findings of on-chain activity. There is less of a need for consensus gathering and formal recommendations given the lack of MEV activity found. Instead, we are prioritizing speed of execution and analysis to improve the committee's performance as a fact-finding arm for the community.

Dashboard Migration

Skip's dashboard has been migrated to Rockaway's Observatory hub. Given the amount of time spent collecting validator data, which was already being compiled by Rockaway, this migration should simplify our processes for identifying validator-related issues. The new dashboard is now live, and includes with it more data gathering tools (e.g. block level analysis).

Updates including data findings and on-chain trends will be published monthly. Keep an eye out for our August report coming soon!