Committee Background

The MEV committee, funded by grants, is an initiative to help the community enforce a social mitigation strategy against malicious validators. dYdX v4 introduced in-memory orderbooks, which allows for malicious MEV activity by block proposers, including frontrunning and censoring user orders. If left unchecked, malicious validators could cause significant harm to the user trading experience.

The committee launched in December following a successful proposal to adopt a social mitigation strategy for preventing proposer MEV, which involves taking out-of-protocol action. By analyzing block-level activity and using Skip's dashboard and protocol metrics, the community can identify malicious activity and take retroactive actions against the responsible actor. To improve the likelihood of catching the activity, and present a more credible threat to bad actors, the committee was assigned to monitor and present findings to the community.

This is our first report to the community, outlining additional context for understanding MEV, our work done, on-chain findings, and future plans.

MEV Background

Before we dive in, here's a quick background on how we define and measure MEV on dYdX v4.

In dYdX v4, there are two types oftrades: short-term and stateful. Short-term orders, like market orders, are peered across the network for execution within twenty blocks without being stored in state. Stateful orders, like limit orders, are recorded in the protocol and accessible to all validators/nodes consuming network data. Due to network latency, not all validators see the same outstanding orders at the same time. Validators in Japan might see a market order to sell BTC at block N that doesn't reach a validator in Europe until block N+1 (or more).

Validators propose blocks that include matching eligible orders (e.g. pairing a market order to sell BTC with the best limit order to buy BTC). Other validators validate these operations, but don't concern themselves with any inclusion or timing details for orders involved. As such, validators can technically choose which orders to match and how before submitting a block. While honest validators use the standard matching system in the v4 codebase, malicious ones might use custom clients to manipulate matching for personal gain. This manipulation of order matching is how we define MEV on dYdX v4. At its core, MEV on v4 involves purposefully changing expected order matches in a block to generate profits for one or more trading accounts (known as user 'subaccounts').

To measure this MEV, the dYdX Research team developed a method for comparing the expected matches from an honest node with those submitted by the proposer. The honest node runs the standard matching algorithm, and measures the PnL output across all subaccounts included in orders matched. The same is done for the orders matched by the block proposer. We can then compare the PnL numbers to find any significant discrepancies across subaccounts. When discrepancies are found, we can analyze the matches further to determine whether an honest issue occurred (e.g. latency) or the proposer is maliciously changing the orders.

These measurements are being tracked by Skip on their dashboard:https://dydx.skip.money/

For a more technical breakdown of how MEV is measured, take a look at the v4 codehere.

What have we been up to?

Since launching a month ago, the committee has been keeping track of on-chain activity through Skip's dashboard while building the tools to analyze discrepancies. The work so far has included:

1. Spinning up a non-validating full node to track block-by-block metrics including order matches and MEV measurements.
2. Developing a real-time monitoring dashboard that uses the node's data for MEV block alerts and quick analysis.
3. Creating a process for deep diving into MEV activity.

Below, we'll outline our current process:

Monitoring

We use Skip's dashboard and our own alerting system to monitor block activity for any MEV events.

While our node's metrics are helpful for analysis, Skip's data is a more reliable source of truth for MEV activity. Skip employs multiple nodes that peer across a wide set of nodes to determine the probability that a discrepancy originates from MEV instead of latency or noise. Our single-node setup with a smaller peering set may lead to higher reported MEV (e.g. missing activity observed by the proposer). Any activity reported on our node is cross-referenced with Skip's data for accuracy assessment.

This blog post is a helpful resource for understanding Skip's process for eliminating noise:Distinguishing MEV from

Expected Noise

Analysis

If Skip, and our node via cross-reference, report events of high MEV, we dig into the block's data using on-chain metrics and Numia's mempool data.

The node's metrics are used to identify the markets, subaccounts, and fill amounts included in any discrepancies found. Using this data, we can reconstruct the orderbook and identify eligible orders using Numia's mempool table, a table that indexes transactions before they are committed to a block. This data allows us to target the timing and sequencing of orders before they're matched, improving our understanding of any malicious intents.

Equipped with these data points, we can determine the origin of MEV activity reported (e.g. an order at a worse price was used, or an order was submitted at the last microsecond). From there, we decide if the proposer is acting maliciously or not.

Analysis Example

To help the community understand our process, we'll share a recent example of MEV activity flagged by our node and Skip.

(a) Monitoring

Our node identified a block proposed by Purple Fog with $163 of MEV captured at height4869848 (01/01/2024 21:09:42). Cross-referencing Skip's dashboard, we see they also found the validator to have roughly the same amount of MEV on that block. With that, we assume a higher probability that this block includes some MEV, prompting us to investigate further.

(b) Analysis

Analyzing our node's data provides more information on the block. The proposer's matches for clob_pair_id 29 (SEI/USDC) don't align with the matches our node expected.

[

1600×530 62 KB

](https://europe1.discourse-cdn.com/standard21/uploads/dydx/original/2X/5/5bcf28c055dfe4403e5b5d3d45448d3fd353071c.png)

[

1290×140 14.9 KB

](https://europe1.discourse-cdn.com/standard21/uploads/dydx/original/2X/a/a351e137ac81bc2d7b8b1ebb7124a9957e45cd14.png)

We can also pull the data directly from the node, which returns the followingJSON. Screening through the 'validator_mev_matches' and 'bp_mev_matches' results, we find that our node expected the block to include two fills between a taker and maker, while the proposer only submitted one.

Node Fill #1:

{"taker_order_subaccount_id": {"owner": "dydx17cyzu9lmhszszspy33jtk6adgzkaunksr4eedt"}, "taker_fee_ppm": 500, "maker_order_subaccount_id": { "owner": "dydx14dltc2w6y3dhf0naz8luglsvjt0vhvswm2j6d0"}, "maker_order_subticks": 7348000000, "maker_fee_ppm": -110, "clob_pair_id": 29, "fill_amount": 1360000000}

Node Fill #2:

{"taker_order_subaccount_id": {"owner": "dydx17cyzu9lmhszszspy33jtk6adgzkaunksr4eedt"}, "taker_fee_ppm": 500, "maker_order_subaccount_id": {"owner": "dydx14dltc2w6y3dhf0naz8luglsvjt0vhvswm2j6d0"}, "maker_order_subticks": 7468000000, "maker_fee_ppm": -110, "clob_pair_id": 29, "fill_amount": 685000000}

Instead, the proposer submitted just one fill:

Proposer Fill #1:

{"taker_order_subaccount_id": {"owner": "dydx17cyzu9lmhszszspy33jtk6adgzkaunksr4eedt"}, "taker_fee_ppm": 500, "maker_order_subaccount_id": {"owner": "dydx14dltc2w6y3dhf0naz8luglsvjt0vhvswm2j6d0"}, "maker_order_subticks": 7468000000, "maker_fee_ppm": -110, "clob_pair_id": 29, "fill_amount": 2045000000}

Though the fill amounts both sum up to equal 20,450 SEI, the taker's purchase is at a worse price in the proposer's fill since it was done entirely at price $0.7468 instead of being split between $0.7348 and $0.7468.

With the root cause found for the discrepancy, we can ask ourselves: was this done intentionally? Did the proposer purposefully fill the taker's entire order at a higher price to generate more value for the maker?

To answer this question, we turn to Numia for additional data. Using their mempool table, we can figure out when these orders were submitted. The timing of orders will matter a lot when it comes to determining the proposer's behavior.

Through this query, we're able to pull the followingdata. In it, we see that the maker's order to sell 13,600 SEI at the better price of $0.7348 was submitted after the order for 66,950 at $0.7468. Given Numia's timestamps, we can even assume the order was submitted as the block was being processed by the proposer.

In conclusion, we can comfortably chalk this up to peering latency and order timing. The new order arrived as the proposer was preparing their block. That was enough time for our node to pick up the order, but not enough time for the proposer to include it in their block.

Contextually, this also doesn't resemble malicious behavior. The order to sell at $0.7348 was submitted after the order to sell at $0.7468 by the same account. Even if the proposer controlled this subaccount, they would have no incentive to submit an offer at a lower price since they were already getting filled higher.

What's happened on-chain?

As of today, no significant MEV activity has been spotted on dYdX v4.

In the past month, we did occasionally witness above average spikes of activity across a number of validators. However, the dYdX Research team found the cause to be with the calculation method, not malicious activity. In short, the MEV calculation formula makes use of the market's mid-price (the price between the best ask and best bid) to measure the PnL for each subaccount. However, given a lack of liquidity and wider spreads on long-tail markets, some mid prices reported were misrepresenting the amount of possible MEV captured. As a solution to the problem, the team patched the formula to use the market's oracle price whenever spreads are above 1%. Since the change was added, we haven't seen any major spikes in MEV activity.

We also saw a few MEV spikes yesterday. We're still in the process of reviewing the data, and we'll report back on any major findings. As of right now, we can assume this is mostly a result of higher than usual trading volume paired with severe price volatility.

What's next?

Looking ahead, we have plans to make our data accessible to the community, such that anyone could perform the same analysis. In the meantime, we'll continue exploring on-chain activity, keeping our eye on any MEV event, and improving our tools for better analysis.