co-authored with @MylesOneil and @Derek

dYdX v4 will use an in-memory orderbook design that may allow block proposers to performMEV. This malicious behavior would come at the expense of dYdX users and the protocol's trading experience.

To protect users, we think it's important to proactively mitigate opportunities to benefit from MEV of any kind. Social slashing is one way to accomplish this goal, which would involve punishing validators who engage in any malicious behavior.

Social slashing can be enabled through a method of reliably detecting MEV activity, combined with a governance-based approach to evaluate and punish bad actors. As described in prior blog posts, MEV activity on v4 can be detected through Skip's orderbook discrepancy dashboard. Combined with a slashing review committee and the power of governance, the protocol can take a proactive stance against malicious MEV extraction.

In this post, we explain why MEV is a threat and what a potential solution might look like. The post should also serve as an invitation to discuss MEV on dYdX more broadly. Given that v4 is expected to launch in late September, we think it's worthwhile to kick off discussions early and start gathering thoughts today. MEV is an important issue that will affect all dYdX stakeholders – we encourage you to share your thoughts.

—--

Background

First, a quick explanation of why MEV is a problem on dYdX v4. Through the in-memory orderbookdesign, validators have an opportunity to reorder or censor trades before proposing a new block to extract profits. These actions wouldn't break anything in the consensus process; other validators would only see the final orderbooks and order fills. In other words, there is nothing within the protocol to prevent validators from engaging in order manipulation as a form of MEV. Given dYdX facilitates billions of dollars of trades daily, we can assume that validators stand to gain a lot of money from doing this, and users lose a lot on the other side.

Based on what we know, dYdX v4 is set to launch with no in-protocol solution for mitigating MEV. In this world, the protocol would be at risk of validators deploying MEV strategies that can pose a significant threat to the trading experience of dYdX users.

As an appchain, dYdX does have the ability to take a more proactive stance toward mitigating MEV. Unlike general purpose chains like Ethereum, Cosmos chains are dedicated to a single application, allowing them to be more opinionated on which behaviors to incentivize (and disincentivize), all enforced through on-chain governance. MEV is one area where app-chains can take a proactive stance, with Osmosis setting an example of a community signaling in support of MEV mitigation.

Social Slashing

In order to address the problem of MEV, the dYdX community can adopt a governance-enforced social slashing model to 'disincentivize and punish bad actors'. In this model, the community can take retroactive action against infringing validators engaged in malicious MEV. Punishment could take shape in a few different ways: it could involve reputation based punishments (e.g. publicly highlighting negative actions by validators and encouraging undelegation), and/or a more direct approach of slashing a validator through governance.

The social slashing mechanism presents a credible threat to malicious validators by retroactively punishing undesired behavior. Profit earned from MEV is now clouded by potential losses from slashing and reputational damage. The validator has to think twice before trying any funny business.

Measuring MEV

How do we measure MEV and catch these bad actors?

Using the dashboard built by Skip, the community can look for orderbook discrepancy among active validators as an indication of malicious behavior. Skip measures discrepancies by deploying multiple nodes that construct orderbooks the same way block proposers do. When a block proposer submits the matching orders of an orderbook, Skip compares that orderbook against their own, which is constructed honestly based on all trading orders published. We can assume that any material divergence in orderbooks, once normalized for network jitter (which the dashboard accounts for), is a result of malicious MEV activity performed by the proposing validator.

[

888×499 367 KB

](https://europe1.discourse-cdn.com/standard21/uploads/dydx/original/1X/1934fabfd22c9e64aafee373ef5cbe5c921fdb15.png)

All discrepancies are measured and assigned to the proposing validator on the dashboard. As these accumulate over the time, the community can identify offenders with above average orderbook discrepancy. A completely honest validator set should display little to no divergence on the dashboard.

To help test the dashboard, the dYdX Trading research team has beenrunning a malicious validator on testnet. The validator employs a sandwiching strategy that manipulates orders to capture MEV. This is exactly the kind of behavior that we would want to catch and punish to protect the integrity of dYdX v4. The dashboard has successfully captured the behavior, with the malicious validator displaying noticeably higher discrepancy compared to other validators. Using this data, the community could take action on the validator by proactively recommending undelegation or potentially slashing their stake through governance.

[

1095×627 57.2 KB

](https://europe1.discourse-cdn.com/standard21/uploads/dydx/original/1X/c16b17a4066922f8d44b7b7b7aff5a810d1abf4b.png)

However, as pointed out by the research team, some minor discrepancies could also appear due to validator latency or other networking issues. There could be false positives in the context of identifying malicious MEV. The community should be careful to review discrepancies such that honest validators are not mistakenly punished for these false positives. We also expect ongoing improvements to the dashboard to reduce such instances. Significant divergence should only ever occur in the event of active manipulation. Any honest validator, even those with occasional latency or networking issues, should not expect to rank highly on the dashboard.

Slashing Review Committee

How can the community efficiently enforce social slashing?

A slashing review committee, made up of qualified community members, can be assigned to proactively review the discrepancy data and recommend action based on their findings. We believe that a committee can accomplish two important goals:

1. Pose a credible threat to malicious validators through proactive enforcement
2. Protect honest validators from false positives

The community as a whole may not be able to catch malicious actors efficiently given coordination constraints. By delegating that responsibility to a committee, validators now know that a group of qualified individuals is actively monitoring their behavior for malicious intent. This introduces a threat of swift retroactive action to malicious actors.

Similarly, the community may be quick to pull out the pitchforks at any sign of discrepancy. However, some discrepancy could be the result of non malicious activity, like network latency or improper maintenance. The committee can be responsible for conducting in-depth assessments, both on-chain and off-chain, to determine the nature of a discrepancy. Based on these findings, the committee can put forward a recommendation for action, with the final decision ultimately up to governance.

With that in mind, we envision the committee adopting the following process:

1. Review all discrepancy data on a regular cadence (e.g. weekly).
2. If a noticeable discrepancy is found, the committee initiates a review process on the validator. The review will include:
3. In-depth analysis of the orderbook data
4. Off-chain inquiry on the validator, which if possible can involve engaging the validator directly to identify the source of discrepancy
5. The committee will report to the community their findings and include a recommendation for action (or inaction). The severity of recommendations will vary based on their findings. In the early phase of implementation, we expect slashing to occur only in the event of egregious and repeated offenses. Proactively undelegating is the expected outcome for most early instances of discrepancy.
6. If needed, the committee will submit a governance proposal based on their initial recommendation and overall consensus from community discussions.

A future version of social slashing may leverage historical discrepancy data to adopt a standard methodology for slashing conditions and severity tiers (e.g. 5% slash if 10bps divergence). If a validator meets certain thresholds for discrepancy, an automatic proposal can kick off to enforce retroactive action based on the severity. The committee could still play a role in catching false positives, veto-ing proposals within a given period of time to stop honest validators from being slashed. The goal is to gradually reduce the subjectivity of slashing standards.

[

500×841 351 KB

](https://europe1.discourse-cdn.com/standard21/uploads/dydx/original/1X/3b3e4508afd90ea6ef5b4f3f356f3f245bfbbdf2.png)

For now, we think a manual approach through an appointed slashing committee accomplishes our goal of imposing a credible threat to bad actors. Naturally, the committee must consist of unbiased members of the community that gain nothing from slashing a validator.

Closing Thoughts

Implementing social slashing requires on-chain data gathering, off-chain coordination, and then governance action – all done retroactively to punish bad actors. While this is not the end game for MEV protection, it's a big step in the direction of mitigating MEV on dYdX v4. We firmly believe that social slashing is the best option available to protect dYdX v4 from harmful MEV activity at launch.

The threat of being slashed, or of being shut out of the protocol, is a powerful deterrent to stop validators from thinking about MEV. Active validators will think twice before engaging in MEV, and delegators will be more careful in their delegation choices. Ultimately, the goal is to build an efficient, but credibly neutral threat to validator economics that puts into question any potential profit earned from malicious activity.

—---

We'd love to hear the community's feedback and thoughts on this post, but also MEV more broadly. Any community-based slashing mechanism should be done with feedback from all stakeholders, whether it's users, tokenholders, validators, or market-makers.

Here are some open questions to kick off discussion:

1. How do you feel about MEV on dYdX v4 overall?
2. What do you think about a social / governance approach to mitigating MEV?
3. How do validators feel about being at risk of slashing for MEV? Is it possible that we deter honest validators from participating on v4?
4. Should we appoint a social slashing committee to review activity on behalf of the community?

Resources

MEV Blog Post #1:

dYdX v4 and MEV

MEV Blog Post #2:

An update on MEV - Catching a Bad Validator

Skip's Order Book Discrepancy Dashboard: https://dydx.skip.money/

Chorus One's MEV Research Report: MEV on the dYdX v4 chain

dYdX Technical Architecture: v4 Technical Architecture Overview - dYdX