Summary

- dYdX v4 will use an in-memory orderbook design that may allow block proposers to perform MEV. This malicious behavior would come at the expense of dYdX users and the protocol's trading experience.
- With no in-protocol solution available, we propose adopting a social slashing strategy to mitigate MEV. The strategy will leverage Skip's dashboard to monitor on-chain behavior and catch bad actors.
- The proposal includes appointing a committee to proactively review data and put forward recommendations. The committee will act on behalf of the community to pose a credible threat, but final decisions are still presented through governance.
- By end of term, the committee will present a framework for standardizing retroactive action based on data gathered.

Background

dYdX v4 is set to launch with no in-protocol solution for mitigating MEV. The protocol may be at risk of validators deploying MEV strategies that can pose a significant threat to the trading experience of dYdX users.

Through the in-memory orderbook design, validators will 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

As an appchain, dYdX does have the ability to take a more proactive out-of-protocol stance toward mitigating MEV. The community can be opinionated on which behaviors to incentivize (and disincentivize), all enforced through on-chain governance.

Description

We propose that the community adopt a governance-enforced social slashing model todisincentivize MEV activity. In this model, the community can take retroactive action against validators engaged in malicious MEV. This presents a credible threat to validators and their delegators. Profit earned from MEV is now clouded by potential losses from slashing and reputational damage. The validator has to think twice before engaging in MEV, and delegators have to think carefully about where they delegate their tokens.

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. These nodes 'determine whether the block proposer has extracted MEV by comparing the observed value to the expected level'. It does so while correcting for networking and latency issues, or noise, improving the likelihood that any discrepancy measured is the result of dishonest behavior.

The dollar value of discrepancy found is measured and assigned to the proposing validator on the dashboard. As these accumulate over the time, the community can identify offenders with above average discrepancy. Similarly, spikes in discrepancy may indicate valuable one-off MEV opportunities being captured by validators. A completely honest validator set should display little to no divergence on the dashboard.

The community as a whole may not be able to catch malicious actors efficiently given coordination constraints. Instead, we propose assigning that responsibility to a committee made up of qualified community members. This committee will be responsible for proactively investigating and reviewing the discrepancy data and recommending actions 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

An active committee introduces a credible threat of swift retroactive action to malicious actors. It also allows for honest validators with potentially false positive data to avoid undeserving punishment. The committee will conduct in-depth assessments, both on-chain and off-chain, to determine the nature and severity of a discrepancy. Based on these findings, it will put forward a recommendation for action (or no action), with the final decision ultimately up to governance through a proposal.

Implementing a framework for action today is tricky given the lack of genuine network activity and trading on dYdX v4. There is no incentive for testnet validators to test out malicious behavior. As mainnet activity becomes better understood, and data is gathered, the committee can leverage their analysis to present a more formal framework for responding to discrepancies. The goal is to gradually minimize the dependency on one-off recommendations by adopting a standard for retroactive action. The committee can learn from the initial launch data and develop a framework that makes sense, which would be adopted through a separate governance vote. Instead of proactively reviewing, the committee can then shift to veto governance –

vetoing actions on false positives or questionable discrepancies to protect honest actors.

Ultimately, it's important to remember that the community will have full control over any retroactive action taken against its validator set. The committee is assigned to improve the effectiveness of data analysis and monitoring. It will act as a relay for recommended action, which may or may not be implemented by the community based governance.

Specification

The MEV Slashing Committee

Members:

7 individuals

Term:

6 months

Budget:

$84,000 ($2,000 / month Member)

Responsibilities:

- Recurring review meetings to discuss MEV activity (starting with weekly)
- Proactively reviewing discrepancy data for outliers and possible MEV activity
- Making periodic recommendations for community action based on findings
- Publishing reports on findings and overall network observations
- By the end of term, the committee should bring forward a framework for standardizing certain actions based on discrepancy data. This framework will be voted on by the community through governance.

This project will launch with the understanding that the committee's exact scope of work will depend on mainnet activity. The exact workload could range from weekly meetings with no further requirements (e.g. there is no MEV activity observed), to a large amount of research, investigations, and governance activity (e.g. MEV is actively observed on mainnet). This uncertainty should not prevent us from moving forward – the downside risk of MEV activity is too large to leave unchecked. A lack of MEV activity found could also be the result of a successful strategy mitigating malicious actors from engaging in the first place.

Members

The committee members will play a big role in the credibility of this strategy. It's important that all stakeholders feel comfortable with its members, including our validators. Validators will be subject to action recommended by this committee with potentially long lasting consequences. We must guarantee that only in the event of malicious activity should validators feel threatened by the presence of this committee.

We believe the following qualifications present an ideal member:

1. Reputation

Members should have some existing reputation at stake, similar to that of our validators. Reputable members are more likely to act honestly and thoughtfully in their decisions. Assuming at least one member is honest with a reputation at risk, the committee's integrity should be upheld. Bribes from malicious validators, or other dishonest behavior, would be mitigated.

1. Knowledge of MEV

Members should have a good understanding of MEV and its role in the ecosystem. By understanding MEV and the strategies employed by actors, members will be better prepared to accurately assess the data. We can expect better recommendations from a knowledgeable committee.

1. Conflict-free

No member should have a pre-existing conflict with a validator or other relevant stakeholder. A member should not have any reason to provide favorable treatment to an active validator. Similarly, there should be no incentive to take action against a validator. We must guarantee a credibly neutral committee that has nothing to gain beyond benefiting the dYdX protocol with honest behavior.

With that in mind, we propose assigning the following members for this initial term:

- Thomas Cintra (Xenophon Labs)

Thomas has been publishing quantitative research for dYdX since early 2022 while working at Xenophon Labs. In this time, Xenophon's research on dYdX v3's Trading Rewards, LP Rewards, and Safety Staking modules have all led to successful governance proposals. On dYdX v4, we've been diving into solutions to mitigate MEV via TEEs and tuning rewards parameters to minimize the profitability of wash trading.

- Udit Vera (Timewave Labs)

Udit Vira is a co-founder atTimewave, a team specializing in developing tools for DAO cooperation, resource allocation, and MEV and governance supply chains. He is also a member of Hypha Coop, focusing on testing, go-to-market strategies, and operational aspects for Replicated Security within the Cosmos Hub.

- Apriori (Heliax / Anoma)

Apriori works with Heliax on Anoma. You can find some of their contributionshere. They have written extensively on MEV and related topics.

- Nitesh Nath (DFlow Protocol)

Nitesh is the founder of DFlow, a decentralized protocol built with the Cosmos SDK that helps wallets maximize revenue, deliver better prices, drive user growth with order flow auctions, and reabsorb the leakage of MEV for their users. Nitesh was previously a quantitative researcher working in high-frequency trading.

- Michael Neuder (Ethereum Foundation)

Mike joined the Ethereum Foundation research team in March to work on Proposer-Builder Separation. He has spent time understanding out-of-protocol solutions (mev-boost and its extensions) and has contributed to the in-protocol design space.

- Craig Le Riche / "0xCLR" (Considered Finance)

Craig has published multiple data driven research frameworks for dYdX, including increasing the maximum funding rate bound research which led to a successful governance proposal and a dashboard built using the risk parameter framework developed. Craig previously managed an OTC market making desk.

- Reverie Reserves, LLC

Reverie is an investment and advisory crypto firm, and active contributor to the dYdX protocol. Reverie has played a role in two dYdX subDAOs – Grants and Ops – and now serves as a Grantor for the Grants program. They have previously funded research and solutions for MEV on v4, helping pave the way for this social mitigation strategy.

Operational structure

We suggest leveraging the dYdX Grants program to issue compensation and monitor deliverables. Using grants to distribute funding lessens the operational overhead associated with additional multi-sigs, payment streams, and governance proposals. The program is equipped to distribute monthly payment based on milestones, and to hold the committee accountable for deliverables.

The Trustees can issue a grant for the full term and distribute monthly compensation to each Member appointed. Given Reverie's involvement with the Grants program, we propose structuring Reverie's compensation as a lump sum retroactive grant to be paid at term end. This allows Reverie to participate in the committee while avoiding a conflict of requesting periodic payments. Instead, the Trustees can decide independently at the end of term if Reverie has fulfilled its responsibility in the committee, separate from its work with grants.

Slashing Proposals

The Cosmos SDK does not inherently support governance proposals to slash validators. Through this proposal, the community is also signaling support for slashing proposals to be added to dYdX. The grants team could explore opportunities to add this functionality through a separate grant.

This change would be submitted through a pull request to the dYdX Chain codebase. Ultimately, adding support for slashing proposals would need to be approved through a separate dYdX Chain proposal to upgrade the protocol to a release that includes these changes.

The MEV Slashing Framework

Ideally, social slashing is implemented through a set of criteria defined using data from Skip's dashboard. We could eliminate most of today's subjective decision-making in retroactive actions by adopting rules that lay out the steps for community action – for example:

- Public notice on a validator if a one-off MEV spike is identified
- Undelegate from a validator if their average orderbook discrepancy is $X or more
- Slash stake from a validator if their average orderbook discrepancy is $Y or more
- Tombstone a validator if their average orderbook discrepancy is $Z or more

However, we first need to collect mainnet data to get a better understanding of the average metrics and MEV events on dYdX v4. The testnet data seen so far could be misleading, especially since we don't expect any testnet validators to be malicious (no incentive to do so). Instead, we propose that the committee members develop a framework based on their findings throughout this first term. The framework would include guidelines for how the community should respond to given data, reducing the dependency on a committee for efficient action.

By the end of this term, the committee will share their findings for standardizing MEV data interpretation. Based on the findings, the committee may submit a formal framework, which the community can vote on to decide whether or not it should be used for future MEV slashing conditions.

Proposal

We propose that the dYdX community signal intent to socially govern malicious validators on dYdX v4. The community will elect a slashing committee to proactively review data and recommend community action, which is to be funded through the Grants program. By approving this proposal, the community would signal a willingness to vote on, and carry out, proposals for retroactive action recommended by the committee. The approval would also serve as community endorsement for the committee members outlined in this proposal. By the end of this initial committee term, we expect the community to vote on a more formal framework for standardizing retroactive actions against malicious validators.

With v4 approaching and recent upgrades to the dashboard completed, we think now is the right time to implement social slashing as an MEV mitigation strategy.

Frequently Asked Questions

1. Why can we not solve MEV directly within the protocol? Why do we need this socially-driven approach?

A formal, in-protocol solution will most likely require some changes to the consensus mechanism of the dYdX Chain. Both leading candidates for in-protocol solutions, Vote Extensions and Trusted Execution Environments, require changes to the way validators process orders and new blocks. As of today, the impact to the chain's performance and trading experience from those changes outweigh the benefits of solving for MEV. We are actively working on improving these solutions through research and grants. Until then, a socially-driven approach can protect the protocol while maintaining the chain's performance.

1. Why is a committee needed? Why can't the community manage this process?

The approach is successful if a credible and efficient threat of punishment is present to deter malicious actors. The committee will actively review activity such that the community has enough time to respond with action before validators and stakers can unbond their tokens. Similarly, the committee's collective reputation adds credibility to recommendations put forth. We can trust them to make careful decisions, knowing their reputations are at stake.

The community will have final say over recommendations through forum discussions and on-chain proposals.

1. What are the risks involved with this approach?

The are two main risks to a social mitigation strategy:

- The solution doesn't work (e.g. it's too hard to manually catch MEV) and MEV happens on the dYdX Chain.
- An honest validator is punished as a result of false positives.

Based on testnet, we expect this solution to work, but things may change on mainnet. We'll need to collectively review the solution on an ongoing basis to determine its success in catching and punishing malicious actors.

Incorrectly punishing honest actors is by far the biggest risk. We must at all costs avoid damaging the reputation of a non-malicious validator, and prevent honest or unknowing stakers from being slashed for no reason. The committee's role will be to carefully review the data, and only make recommendations when it's absolutely clear that MEV activity is present.

1. Why is Skip not directly involved with the committee?

Skip will work closely with the committee to provide data and context on the findings, but remain a neutral service provider throughout the process. The committee will be equipped to make accurate recommendations, but also have the independence to cross-reference data through other means. The integrity of the committee is upheld by serving only to solve this problem for the community.