# Executive summary

This post is a response to Lido's call for an MEV policy. It proposes that Lido outsource block building to mev-boost, a decentralized market for full block templates, and make it mandatory for all NOs. This policy maximizes staking APR for Lido, maximizes Ethereum security, minimizes the risk of MEV hiding, and reduces Lido's ability to pressure NOs in adversarial ways (which, as we show, is a very good thing.)

# Disclosures

mev-boost is developed by Flashbots in close collaboration with the Ethereum Foundation. I lead Strategy at Flashbots. I am also Strategic Advisor and an investor at Lido.

# Table of contents

# What is mev-boost?

mev-boost is an implementation of a technique called proposer-builder separation (PBS). It isolates the increasingly specialized role of block builder, who creates the block template, from proposing the block in consensus. PBS is rolled out to Ethereum in three stages. Stage 2 PBS, called mev-boost, introduces a competitive market where many builders can compete to buy blockspace from validators, thereby maximizing revenue for the seller and making MEV available. mev-boost is developed by Flashbots in close cooperation with the Ethereum Foundation and will be enshrined in the Ethereum protocol in the future (Stage 3 PBS). Read more about mev-boost here.

# What does the optimal MEV policy for Lido look like?

I believe that the right MEV policy is a matter of optimizing the following dimensions:

[

lido policy

1068×707 134 KB

](https://europe1.discourse-cdn.com/business20/uploads/lido/original/2X/e/e766cd18d71aa881adf986313ab4feeb18f4b8a3.jpeg)

## Maximize Staking APR

Extracting all available MEV is good for Lido because Lido competes for stake from users on the one side and quality NOs on the other. Both are maximized when staking APR is maximized. Under an alternative policy that doesn't maximize APR, stakers would be more likely to delegate to a different provider, and NOs would be more likely to circumvent Lido and market to users directly, and/or participate in Lido but attempt to extract the MEV in a hidden way and hide the rewards from Lido/stakers (see "MEV hiding".)

## Maximize Ethereum security

This policy is also optimal for Ethereum's security becauseMEV must be extracted for economic security: "A system where validators "leave MEV on the table" is one where an obvious attacker subsidy is readily available. This is self-defeating and degrades security in a pure-economic-rationality model, as it causes centralization/oligopoly." To make blockchains maximally robust, all honest actors need to extract MEV at the maximum rate, otherwise they dramatically lower the cost for a dishonest actor to attack the system.

## Minimize MEV hiding

The mev hiding problem is defined as follows: Lido NOs handle the staking in return for 5% of the overall staking reward. However, because NOs can receive money in direct transfers or off-chain, this number carries a lot of uncertainty. Lido can ensure it gets 95% of the rewards it can see, but not of the rewards it cannot see.

For example, a scenario where NOs report 1 ETH reward per block to Lido (of which they receive 5%) but hide 0.5 ETH reward from Lido (of which they get to keep 100%). This is a large carrot for NOs at the expense of Lido and its stakers.

The ability to steal decreases the more Lido's confidence about the true size of the reward increases. In other words, it is an oracle problem. Staying with the above example, if Lido knows the true value of the block is 1.5 ETH, the NO can still try to report 1 ETH to Lido, but the theft would be easily detectable.

To resolve the mev-hiding problem, you need a reliable oracle on the true block reward. This value is provided by the clearing price of a competitive market for full-block templates. In such a market, builders have to make wholesale bids for blockspace to validators. To maximize their chance to win, these builders have to maximize their public bids in order to win. the example block that e.g. bids 1 ETH in public and hides 0.5 ETH in private will not be competitive in this market.

As long as validators sell their blockspace to the highest-selling bidder, there is high confidence that NOs are not engaging in value hiding on the side.

## Minimize power over block building

Parts of the Ethereum community, and evenselect core developers, have argued that Lido's control over block production poses a risk to Ethereum security. The argument goes like this: Lido can exercise soft power over NOs via the whitelist. They can use this pressure to censor Ethereum users, reorganize the network, or extract monopoly prices from users.

These concerns have createdexternal pressure on Lido to self-limit its growth, which is ultimately bad for everyone: It allows centralized competitors to catch up, leads to more fragmentation in the staking tokens market, and reduces revenue for LDO holders. The underlying problem is not that Lido wants to hurt Ethereum users but that it can't prove that it doesn't — a trust problem. The lesson for Lido is that the more it can reduce its control over the protocol, the bigger it can scale, and the more money it can make. Building on this principle, Lido has developed the Dual Governance proposal. The goal is to minimize the scope of governance (what can go wrong) as much as possible and give stETH holders a veto for the rest.

The same logic should be extended to block building: By requiring that NOs source blocks from open markets, Lido effectively removes the potential for it to coordinate or exercise influence over the content of the blocks being built by its NOs; the less Ethereum users have to trust Lido, and the more Lido can scale.

# Proposal: Adopt mandatory mev-boost for Lido

In this proposal, all Lido NOs would adopt the mev-boost middleware to access the distributed block builder market. A competitive market for full-block templates presents a huge opportunity for Lido. This market is an objective block template source that maximizes revenue for Lido, protects Ethereum, minimizes MEV hiding, and reduces Lido's power over block production. The use of mev-boost would be mandatory for all Lido NOs.

## Monitoring compliance

Lido can measure non-compliance by comparing the most valuable known block template offered on mev-boost (”the reference block”) to the one an NO actually produced. If they differ, the NO was either not using mev-boost or engaging in MEV hiding.

Some leeway should be given to NOs for potential network problems, faulty relays, or buggy software outside their control. It should be enough for Lido to punish gross misbehavior, e.g. if a NO is deviating from the reference block more than 1% of the time over a rolling time window.

Before withdrawals are possible, non-compliant NOs can be cut off from receiving more stake from the DAO. This can be enacted by the DAO via an on-chain vote. After withdrawals, non-compliant NOs can be off-boarded as well.

## Choice of relays

One open question that I want to kick to the community is the curation of relays. This proposal aims to outsource block production to an objective block market.

If Lido allowed NOs to freely choose what relays to connect to, this would violate three of the four goals of the policy (no longer maximizes staking APR or Ethereum's security, and minimizes MEV hiding.) But if Lido enforced an entirely static list of relays, it might give these relays too much power over the builder market. Competition between relays seems desirable so new relays should be able to enter the market and go “from rags to riches”.

A good middle-ground might be for Lido to enforce both a must-include list (standard relays that all NOs must include) and a must-ban list (for adversarial relays that no NO can include.) These lists could be subject to periodic review by the DAO. Under extreme circumstances (e.g. a large centralized builder with exclusive orderflow capturing the entire market and extracting monopoly prices from users), Lido would retain the ability to blacklist builders for the sake of Ethereum.

## Policy maintenance

Proposer-builder separation is part of the Ethereum roadmap and its rollout happens in several stages. Lido's policy should be to use the most decentralized and competitive implementation of PBS. While the final goal, protocol-enshrined PBS, is still a couple of years away, mev-boost is good enough for the time being and, most importantly, is available today.

This policy should be reviewed with some frequency to ensure that Lido remains on the best solution. The review should include how the policy performed against its target objectives, consider available alternatives, and decide on possible changes for the next period. The reviews shouldn't be so frequent that they endanger the goal of minimizing Lido's power over block building. Starting with a period of one year seems fine, and the increasing period length as the block template market ossifies.

# References

Ethereum MEV Extraction and Rewards - Discussion & Policy Groundwork (Izzy)

Why run mev-boost? (Hasu and Stephane Gosselin)

mev-boost Github

MEV… wat do? (Phil Daian)

The Risks of LSD (Danny Ryan)

Should Lido on Ethereum be limited to some fixed % of stake?

LDO+stETH dual governance (Sam Kozin, Hasu, et al)