TL;DR

This a proposal to fund Nethermind to design a Sybil and white-labeling resistance mechanism. The delivery will include a detailed discussion of the final design and a systematization of knowledge for Sybil resistance mechanisms, oracle systems, prediction markets, and token-curated assets. During the project, a dedicated team will investigate what the state-of-the-art is, what solutions are or will be used in practice, and how. Then we will propose concrete mechanisms to make Lido's network Sybil and white-labeling resistant. The project will be one of the steps toward enabling Lido to onboard new operators in a permissionless manner. This is a continuation of our previous proposal. The project will take 28 weeks, and its cost — 700 000 DAI — will be covered by Lido DAO.

Proposer and work mindset

Proposer

Michał Zając on behalf of Nethermind.

About Nethermind

Nethermind is a team of world-class builders and researchers with expertise across several domains: Ethereum Protocol Engineering, Cryptography Research, Layer-2s, Decentralized Finance (DeFi), Miner Extractable Value (MEV), Smart Contract Development, Security Auditing, and Formal Verification, among others.

Our Research team comprises mathematicians and engineers who work on analyzing, breaking, and designing blockchain and cryptographic schemes. Our expertise and interests span the fields of zero-knowledge proofs, non-deterministic programming, Distributed Validator Technology, liquid staking, and decentralized identity.

Working to solve some of the most challenging problems in the blockchain space, we frequently collaborate with renowned companies and DAOs, such as Ethereum Foundation, StarkWare, Lido Finance, Gnosis Chain, Aave, Flashbots, xDai, Open Zeppelin, Forta Protocol, Energy Web, POA Network and many more. We actively contribute to Ethereum core research and development, EIPs, and network upgrades with the Ethereum Foundation and other client teams.

General work mindset

The following principles will drive the development of the protocols:

- All the design considerations and risk analysis will be done with the consent of the Lido DAO.
- Nethermind will set up a dedicated team for this effort.
- All proposed solutions will come with security analysis. When available, the protocols' security will be proven.
- Milestones and deliverables will be small to ensure a good overview of the team's progress.

Terminology

- Operator: A party that runs, or participates in running, one or many Ethereum validators. Operators, solely or jointly, have access to the signing keys of one or more validators but do not necessarily have control of the corresponding withdrawal credentials. Operators can control multiple nodes.
- Node: A virtual sub-party (a piece of hardware and software) controlled by an operator that performs the operator's jobs w.r.t. a concrete validator. When an operator is a party that may control multiple validators, a node is a representation of a concrete validator.
- White-label operators: If a party, who was onboarded as an operator, delegates the operation of a node to another party, we call the latter a white-label operator.
- Sybil operator: We call a party Sybil if it controls two or more operators behind the scenes. A Sybil-protection mechanism is a set of countermeasures that makes it difficult for a party to have two (or more) operators onboarded such that the protocol is unaware they are colluding.
- Protocol score (or score): protocol's internal scoring system that measures whether the operator contributes to the good quality of the set of operators.
- External reputation: operator's reputation in ecosystems external to Lido, e.g., in real life, in Web2 services, in other Web3 services, etc.

- Arbiter protocol: we call a protocol “arbiter protocol” if it is either a decentralized oracle, token-curated asset, or prediction market.

Ideal mechanism overview

An ideal mechanism evaluates Lido’s DAO validator set according to the operator & validator set strategy described inthis note by Lido. More precisely, the mechanism must have methods for improving the validator set if there is an option to do so. It must have zero input from permissioned roles (i.e., no admins/committees). Furthermore, it must have an input of low to zero impact from LDO, stETH, and ETH token holders.

The mechanism has to be capital efficient: Collateral for operators can be used, but it can’t be the single or primary mechanism; it has to function mainly by staking with other people’s money.

The mechanism has to account for the bull-bear cycle effect in a way that would allow operators to stop validating if it becomes too expensive. Additionally, the mechanism has to reduce the number of operators in bear markets and expand in bull markets.

The mechanism has to prevent the set of operators from becoming worse. This includes, but is not limited to, avoiding the following:

- reduced performance,
- reduced neutrality,
- offline time,
- slashable offenses,
- reduced jurisdictional geodiversity,
- reduced localization diversity of the infrastructure,
- reduced Ethereum client diversity and other diversity vectors,
- giving up independence (e.g., in a merger),
- destructive MEV,
- delegation of operation (delegating operator duties should reduce the amount of stake that the operator can control, potentially removing it from the operator set altogether).

Improving operational quality should increase an operator’s revenue (by increasing the stake or the commission).

The stake should be distributed flat-ish. Operators should only control up to 1% of total ETH staked through Lido.

The mechanism cannot overfit on any particular parameter, but most importantly, it cannot overfit on performance: super-performant operators often cut corners or sacrifice specific attributes for others. Furthermore, overfitting performance and profitability is inherently centralizing due to economies of scale and, in general, cost-minimizing (i.e., locating in places w/ the cheapest servers, bandwidth, etc.). That being said, the mechanism has to ensure an overall good level of performance

The mechanism should allow for a new operator to enter the set of operators with essentially no collateral or reputation and work its way to an optimal position within the network of operators. That should be possible, although it may take a long time, if the operator has a “good enough” performance and is ecosystem aligned, independent, and runs its hardware in non-concentrated geographical/jurisdictional areas. There might be a need for an insurance pool or collateral to enter at zero or to rise to the top, but it could be optional in the middle.

The amount of stake controlled by an operator should depend on a "protocol score.” This score should reflect how much the operator contributes to having a good overall validator set. In particular, an operator joining the protocol should be given a low to neutral score, implying that it can control a very limited stake. The score, and thus the amount of the controlled stake, should be increased when contributing to some or all of the following. We note that the exact scoring mechanism is yet to be researched, so the list below is provisional.

1. Providing additional bond.
2. Providing good quality services. Users can build their reputation (and thus score) by providing good services. Defining what “good services” means will be part of Phase 3.
3. Providing information about itself, for example, revealing its Web2/Web3/real-life identity or other credentials such as educational institution diplomas, GitHub activity, hackathon awards, etc. Ideally, this information will be provided in a privacy-preserving yet verifiable manner.

An operator that provides its identity has more to lose than just bond when it misbehaves. Its external reputation is at stake. Additionally, an operator that (verifiably) reveals technical knowledge credentials is more likely to operate its validators properly. In some scenarios, this could increase the Sybil resistance of the network (though this increase is certainly limited, and a complete Sybil resistance solution would need to rely on further mechanisms).

Notably, users who want to remain anonymous would still be able to control a substantial stake by providing bond (Point 1) or gaining a reputation by providing good quality services (Point 2).

General objectives

“We will assist Lido in creating and maintaining a permissionless and high-quality validator set mechanism. This entails:

1. Designing and implementing methods to ensure that validators are run by a high-quality set of operators. In particular, each operator performs its duties on its own and does not cede them to an external party (i.e., it does not hire a white-label operator), nor is secretly associated with other operators, and ensures that its hardware and software run performantly.

2. Conducting a thorough economic analysis to understand how the market fluctuations, or changes in the Ethereum protocol itself, can compromise the system’s security.

The project will be divided into four phases:

- Phase 1:

We survey the literature and state-of-the-art approaches to identity and attestation schemes. This phase has been completed already.

- Phase 2:

During this phase, we will survey the literature and state-of-the-art approaches to oracles, token-curated assets, prediction markets, Sybil, and white-labeling-protection mechanisms. The present proposal focuses solely on this phase.

- Phase 3

: Next, we will proceed to design solutions for assuring a good quality set of operators and economic security of the protocol. We will also describe the resources required to implement the solutions proposed in Phases 1, 2, and 3.

- Phase 4:

This phase is mainly concerned with implementing the solutions designed during Phases 1, 2, and 3. We will also research some extra topics and problems, as done in the previous phases, and afterward, we will implement them. Further information on this phase will be provided later, by the end of Phase 3.

Project Objective

Phase 2. Sybil and white-labeling resistance mechanism design

In this part of the project, we will focus on one of the crucial aspects of the security of a permissionless staking protocol. Namely ensuring that:

1. Operators are separate entities. That is, there are very few parties that control multiple operators secretly, and no party controls the majority of the operators.

2. Operators perform their duties independently and don’t use third parties, so-called white-label operators, to do them on their behalf.

In both cases, an entity that runs multiple operators (whether by controlling Sybils or being a white-label operator) could have too much control over stake, and the protocol in general. This would worsen the overall health of the protocol, weaken its resistance against correlated slashing, and could introduce a single point of failure.

We emphasize that even if we ensure that all onboarding operators are honest, we still need to have a system that detects dishonest parties within the set of already onboarded operators. This is because Sybils/white-label operators can be created among the onboarded operators, even if these operators honestly entered the system. The latter may happen, e.g., when one entity that runs operators buys another that also runs operators. In that case, the buying party may end up controlling too much of the stake.

Our work plan for developing a solution for Sybil and white-labeling resistance will begin by researching several techniques that, we believe, have the potential to lead to a solution in isolation or as part of an amalgam. The different types of methods we will explore are listed below. In particular, we will investigate credential and arbiter protocols. The former could help fight Sybils. The latter could be used both to fight Sybils and detect white-label operators. Namely, a party that suspects that some operator is a white label could raise that issue and make a corresponding prediction market where people can bet on whether they believe in the claim. Then the conflict would be resolved by an assigned resolution mechanism.

The final goal of our work will be to produce a report explaining exactly how the Lido network can use such methods.

TASK 1

Sybil and white-labeling resistance. SoK.

We will begin with supplementing the SoK from Phase 1 with an SoK for Sybil and white-labeling resistance. We will look for such mechanisms used not only in Web3 but also in Web2 and, if necessary, real life.

This part will take 4 weeks.

TASK 2

Limiting Sybils by using credentials.

Operators who wish to control a lot of stake may be willing to use their credentials to ensure they are not Sybils and increase their score by putting their external reputation at stake. To preserve the operators' privacy and limit the system's reliance on the externally issued data, we will propose a mechanism that does not learn or store the credentials but only uses them to ensure that the entity presenting them is not trying to cheat the system. We will use zero-knowledge proofs to protect the users' privacy. In this part of the project, we will rely on the SoK on decentralized identities and verifiable credentials we delivered in Phase 1. We will also discuss how to make it harder for dishonest operators to use credentials unrelated to them (e.g., bought on a black market).

We will propose mechanisms (one per credential type) that may be used to incorporate

- real-life credentials
- Web2 identities
- Web3 identities

to the Lido protocol. To preserve operators' privacy, we will ensure that only minimal information about them is revealed.

This part will take 7 weeks.

TASK 3 Arbiter protocols. SoK.

We expect some core components to be decentralized oracles, token-curated assets, and prediction markets. We will use these "arbiter protocols," as we call them, to assess whether

- a prospective operator will provide good quality services and contribute to the quality of the operators' set or
- an already onboarded operator is Sybil or uses a white-label operator.

As a first step, we will prepare an SoK for the following topics:

- decentralized oracles
- token-curated registries
- prediction markets

This part will take 5 weeks.

TASK 4 Arbiter protocols. Resolution mechanisms.

In this part, we will design a mechanism that resolves disputes in arbiter protocols. We will propose concrete setups for decentralized oracles and prediction markets. We will specify which parties make the oracle and who resolves disputes in prediction markets. We will analyze the feasibility of using already onboarded operators as part of an oracle system. Similarly, we will also explore the idea of using LDO holders as a resolution mechanism for prediction markets and oracles. To protect operators from being unjustly accused, we will design a mechanism that allows such operators to raise a flag and notify the DAO of the resolution mechanism's wrongdoing.

This part will take 8 weeks.

TASK 5 Incentivizing entities to be transparent about the nodes they are operating

In this task, we will design an economic mechanism that incentivizes entities not to hide information about the nodes they are running. While this will not deter highly motivated and malicious operators, it may be enough to prevent many semi-honest or rational entities from creating Sybil accounts. We will analyze the feasibility of designing a robust mechanism. If the feasibility studies are concluded positively, we will propose an incentivizing mechanism that could lead to a more robust system against Sybils. We emphasize that we will require the mechanism to not harm operators' privacy.

We will work on such mechanism for 4 weeks.

This phase will be completed within 28 weeks from the date of the agreement.

Organization, Funding, and Budget

Nethermind will create a dedicated team to run this project.

The project will be funded by Lido DAO. The DAO will pay Nethermind 700 000 DAI, of which 50% (350 000 DAI) will be paid upfront and the remaining 50% (350 000 DAI) on delivery.

At the end of the project, the LEGO council will decide whether the provided systematization of knowledge meets the agreed requirements and, if that is the case, proceed with the payment. In the case of disagreement between the LEGO assessment on the quality of the deliverables and Nethermind, Lido operators will be used as a resolution mechanism.

The payment will be made to address eth:0x237DeE529A47750bEcdFa8A59a1D766e3e7B5F91

Next steps

We want to put this proposal to a vote in 14 days. The voting will remain open for 7 days.