TL;DR

This proposal is to fund Nethermind to deliver a Systematization of Knowledge for Decentralized Identities and Verifiable Credentials. During the project, a dedicated team will investigate what the state-of-the-art is and what solutions are used/planned to be used in practice, and how. The project is one of the steps toward allowing Lido to onboard new operators in a permissionless manner.

The project will take 6 weeks, and its cost — 150 000 DAI — will be covered by Lido DAO.

Proposer

Michał Zając on behalf of Nethermind.

Terminology

- Operator: A party that runs, or participates in running, one or many Ethereum validators. Operators, solely or jointly, have access to validators' signing keys but do not know validators' withdrawal keys. Operators can be divided into 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. to a concrete validator. When an operator is a party that may control multiple validators, a node is its representation for a concrete validator.
- Committee: With DVT (Distributed Validator Technology), multiple operators may jointly run a validator in a distributed manner. We call a committee the set of all nodes assigned to such validator.
- White-label operators: If an operator delegates its tasks to another party, we call the latter a white-label operator.

Ideal mechanism overview

An ideal mechanism evaluates Lido's DAO validator set according to the operator & validator set strategy described in this note by Lido. The mechanism has methods for improving the validator set if there is an option to do so. It has zero input from permissioned roles (i.e., there are no admins/committees). And it has 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 that becomes too expensive for them and for the protocol to contract 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,
- offline time,
- slashable offenses,
- reduced geodiversity,
- reduced Ethereum client diversity and other diversity vectors,
- giving up independence (e.g., in a merger),
- destructive MEV
- delegation of operation has to reduce the amount of stake that an operator can get, potentially down to removing it from the 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. No operator should control more than 1% of total ETH staked (globally).

The mechanism can't overfit on any one parameter, but most importantly, it can't overfit on performance: super-performant

operators often cut corners or sacrifice certain attributes for others. There has to be a “good enough” 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 own 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 shouldn’t be an important requirement in the middle.

Objectives

We offer to help Lido with maintaining a high-quality validator set

. This entails:

1. Designing and implementing methods for assuring 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. the operator does not hire a white-label node), is a proficient DevOps engineer, and ensures that its hardware and software run performantly.
2. Conducting economic analysis to understand how market changes, or changes in the Ethereum protocol itself, can impede the system’s security and how to secure the system against unfavorable market changes.

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. See the Roadmap for Phase 1 below for specific details. The proposal focuses solely on this phase.

- Phase 2:

During this phase, we will survey the literature and state-of-the-art approaches to oracles, token-curated assets, and prediction markets.

- 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. Additionally, we will 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.

About Nethermind

Nethermind is a team of world-class builders & researchers. Our work touches many parts of the industry, from our Nethermind node to fundamental cryptography research and application-layer protocol development.

Motivation

Permissionless operator set

Our research will first focus on ensuring a high-quality set of operators for the Lido network. A light-heartedly created set of operators could put users’ stakes at risk or even threaten the security of the Ethereum network. Hence the method for permissionless and secure operators’ evaluation, addition, and removal is crucial.

Although the whole set of operators should be of high quality, we need to allow newcomers to join the network as well. Newcomers may not have records good enough to be considered of high quality, but they should be able to work their way up to a high-quality status.

Another problem to study is how and when to arrange the operators into committees. Since the network allows newcomers that may be of a lower quality, it is essential from the network’s performance and security perspectives to ensure that high-quality operators have the required majority of voting power in all validators.

Since on-chain data may not be enough to assure a high-quality set of operators, it is important to design a mechanism that

pulls off-chain data on-chain. Here we differentiate two sources of data: issuer data and community data. The former is taken from official institutions, trusted issuers, etc. The latter is taken from distributed communities. It is crucial for the data to be obtainable and verifiable. The quality of data determines the quality of the reputation and quality systems.

Economic analysis

Another crucial part of assuring a good set of validators is to create a robust incentive mechanism that assures that rational actor behave honestly and in a manner that helps shape the operator set according to our design goals (e.g. having operators be as diverse as possible), being this the behavior with the greatest payoff. To that end, an in-depth analysis of liquid staking economics incentivization methods is required.

We also note that an incentive mechanism is needed to obtain good quality data — both to have data pulled on-chain and to have it verified.

We also propose to analyze how users' and operators' incentives change if the proposer-builder separation is included in Ethereum.

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 assure a good overview of the progress the team makes.

Project Objective

Phase 1. Decentralized identity and verifiable credentials. Systematization of knowledge.

- We will start by investigating classical results in Decentralized Identity Schemes and Verifiable Credentials.
- Then we will discuss the recent advancements in these two areas
- Finally, we will investigate what solutions are used in practice (or planner to be used), how projects use them, what are the security assumptions and properties, what are the known roadblocks.

The deliverable will be a systematization of knowledge research survey.

The deliverable will be completed within 6 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 150 000 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.

The payment will be made to address eth:0x237DeE529A47750bEcdFa8A59a1D766e3e7B5F91

Next steps

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