

Building upon our existing [roadmap for adding secret shared validator functionality in Nimbus](#) the Nimbus team is proposing to conduct research into potential improvements to the existing Ethereum DVT protocols with the goal of making the upcoming LIDO DVT offerings maximally robust and [easy to use](#).

Goals

Our research will focus on identifying and proposing missing standards that aim to:

1. Deliver the best possible validator performance.
2. Improve the inter-client interoperability.
3. Facilitate the creation of more accessible and functional client management interfaces.

Deliveries

More specifically, we expect to complete the following deliveries:

- Standardized formats for distributed keystores and keystore shares.
- Keymanager API extensions for managing distributed keystores and keystore shares.
- EIPs featuring precise cryptographic specifications and test vectors for the following processes:
 - Distributed keystore generation
 - BLS threshold signing
 - Keystore shares rotation
 - Distributed keystore generation
 - BLS threshold signing
 - Keystore shares rotation
- LibP2P protocols and Beacon API extensions for coordinating the execution of the validator duties in a variety of trust models.
- Guidelines for the CLI interface of the clients.

Use cases

We believe that any research into DVT should strive to be as neutral as possible and should take into consideration the multitude of benefits and use cases that the technology could bring to:

- Solo stakers and professional operators seeking to improve the resilience of their setups.
- Professional operators seeking to gain protection from rogue employees.
- New staking protocols aiming to distribute the responsibility of operating an Ethereum validator among a group of weakly trusted users.

What differentiates this proposal?

Before standardization, we will explore the problem space through pilot implementations in the Nimbus client that will aim to validate that the proposed standards can achieve the desired performance and robustness. We acknowledge that many of these problems have been addressed in prior art such as the SSV network, Obol, Diva and SafeStake, but none of these project offers a similar breadth of standardization. We intend the leverage the successful practices of these projects, but we will also try to innovate in few key areas:

- Setups for solo stakers and professional operators can leverage the higher level of trust between the nodes of the DVT cluster by taking advantage of more efficient coordination algorithms, derived from Raft.
- We believe that our deeper understanding of the factors (including corner cases) that affect validator performance will allow us to design more robust coordination protocols that are better integrated into the existing BN/VC architecture, and are easier to scale to a large number of validators.

Requested budget

To support this effort, we are requesting 50,000 DAI from the LIDO community, with 50% unlocked upon the completion of

the listed deliveries. This would constitute one third of our projected budget and we are deeply grateful to the Ethereum Foundation and [Ether.fi](#) for their expressed support and encouragement for this initiative.