[LEGO] Proposal to improve security of Lido's Oracle with zkSNARK light client

TL;DR

Lido currently uses a trusted multisig for getting information from the Beacon chain (consensus layer) to the execution layer. Telepathy, a zkSNARK based light client for the Beacon Chain, can be used for trustless access

to consensus layer information in the execution layer without needing an external multisig. Integrating Telepathy into the Lido protocol will significantly improve the security of the protocol

by augmenting the security of the multisig, and be a major step towards decentralization as it provides a path to getting rid of the oracle multisig altogether. Telepathy is live on mainnet and the integration work can start today.

Context

Currently, the Lido oracle contract is used for getting consensus layer information key to the Lido protocol, such as the balances of Lido validators. The oracle relies on a third-party quorum set, which is a 5/9 multisig, to attest to this information. @e-kolpakov previously noted the main consequences of this design inthis post:

Security

: A dedicated and resourceful attacker can work towards acquiring control of the majority of oracle members - and abuse the oracle contract when it is achieved.

** practically this is a 51% attack, however at the moment there are only 5 trusted oracles (see getOracleMembers in the contract), so 51% attack essentially boils down to overtaking just 3 entities. There's a proposal to increase the number of oracle members to 11 - this should make it considerably harder (need overtaking 6 entities), but still within a realm of practically feasible.

Cost

: Contract requires a considerable amount of expensive storage read/write operations to manage members, check if reports are coming from a trusted source, and keep track of reports while quorum is being accumulated.

Scalability

: With the network growing. the cost of quorum calculation grows linearly (O(N)) with the number of trusted oracle members.

Increasing the Security of the Lido Oracle

Succinct has built Telepathy, a zkSNARK-based light client for the Ethereum Beacon chain.

Telepathy light client

The Telepathy light client works by verifying Ethereum's light client protocol (the sync committee). In particular, we verify the signatures of the sync committee in a zkSNARK and verify sufficiently many members of the sync committee have signed off on the current Beacon state. This zkSNARK "proof of consensus" allows us to run a gas-efficient on-chain light client, allowing for trustless access to Beacon Chain information in the execution layer.

View our light client getting updated on mainnet today with consensus layer headers on Etherscanhere.

Lido Validator Information with Telepathy

The Lido protocol needs information about Lido validators (balances, rewards, slashings, etc.) for its operation. Currently the Lido oracle multisig is responsible for attesting to this information that is used by the protocol. With the Telepathy light client, the Lido protocol can now gain trustless

access to information about Lido validators, without having to rely on an external multisig.

By integrating Telepathy, Lido's reliance on an external multisig can be more secure by having an additional trustless source of information. Furthermore, this integration provides a path for the external multisig to be removed entirely, which increases the decentralization of the protocol.

Proposed Integration

The integration of Telepathy into the Lido protocol is relatively straightforward. We will create a smart contract Beacon oracle that uses the Telepathy ZK light client as a source of truth and verifies relevant Lido validator information against the

consensus block headers. If the gas costs of verifying these validator statistics is too expensive to do on-chain, we will zkSNARK the SSZ proofs, which will make the gas costs practical.

Finally, our beacon oracle contract can be added as another member on the current Lido oracle multisig, and with time can perhaps replace the need for an external committee entirely. Our beacon oracle contract would call the reportBeacon(...)

function on the current LidoOracle

contract for a seamless integration in providing addition security to the multisig.

Validator Statistics Examples

Here is an example of how the Telepathy ZK light client can be used to retrieve validator balance data. Another example contract here shows how we prove validator balances and other fields about validators (i.e. validator slashings).

Additional Information

Security

Security and transparency matter to us. Our protocol has three end-to-end audits from top firms: Veridise, Trail of Bits and Zellic, in addition to a bug bounty program. The code is also fully open-sourced: view our Github repository with the zkSNARK circuits here and smart contracts for the zkSNARK light clienthere.

Sync Committee

Our light client protocol is secured by the sync committee, which you can read more about in our docshere and our blog post here. While current bridging solutions are solely secured by a multisig, requiring the sync committee's signature provides Telepathy an additional layer of security.

Current Partners

Succinct has partnered with Gnosis DAO, who are using Telepathy in securing their native bridge (with $XX million in TVL). Across Protocol, a liquidity layer, is partnering with Telepathy to secure sending messages from Ethereum to Avalanche and BSC. Additionally, Succinct is in talks with and integrating Telepathy with several other liquid staking solutions.

Expected Impact

We believe that making the Lido protocol more secure and decentralized is extremely important for the future of the protocol. We believe that this R&D work incorporating a zkSNARK light client for improving the security of the Lido multisig is high-impact as it significantly increases the security of the protocol. Additionally, this work provides a path to eventually not needing the external multisig altogether, which is important for the long-term decentralization of the protocol. We also think this is a good opportunity for the Lido protocol to support external contributors doing important long-term research and R&D.

Deliverables

Our deliverables will be:

- A smart contract Beacon Oracle that will verify Lido validator information against the Telepathy zkSNARK light client block header
- A write-up and blog post of how we computed and verified this validator information in our smart contract. If desired, this blog post can be a collaborative effort between Lido core contributors and the Succinct team.
- An API endpoint to retrieve the relevant information to generate these Beacon Oracle updates for the Beacon oracle smart contract

Grant Amount

The Telepathy zkSNARK light client is has been audited and is already in production on Mainnet today. We propose a 20,000 DAI grant for the R&D work of creating the BeaconOracle

contract that will verify the necesary SSZ-inclusion proofs for the particular validator information that is needed by the Lido protocol. If the gas costs of this method end up being too expensive, then we can revisit additional grants for the work of zkSNARK-ing these SSZ proofs, as that R&D work is more intensive and complex.