TL;DR

Lido stETH stream contributors propose to improve the safety check for the accounting report in the case of a negative rebase, reducing the possible impact size, but with the requirement for a second opinion for extreme cases.

It is proposed to change the current AccountingOracle sanity check, which currently does not allow reporting more than a 5% of Consensus layer validator balance and withdrawal vault balance decrease daily, to a sanity check, which will not allow more than ~3.4% per an 18-day window (1.101 ETH decrease per validator concerning the window).

Motivation

The AccountingOracle contract aggregates all Lido validators' Beacon Chain balances (clBalance

in the report) to the protocol, critical for the daily rebase of the stETH token. It uses a committee of nine Oracle daemons, with a consensus required from at least five, to ensure data integrity.

The protocol could be harmed if this committee is compromised, malfunctions, or colludes. This risk is acknowledged and constrained by a sanity check that restricts the possible discrepancy in balance that Oracle can report. The current approach to sanity checking allows the Oracle committee to bring up to a 5% reduction of TVL in each report. Given that the governance reaction time is 3-4 days, the malicious or compromised Oracles could reduce the TVL by 15-20%, invoking mass liquidations on lending markets and dropping the price of stETH.

However, a real negative rebase has very distinct features that can be taken into account to reduce the impact and attack surface while allowing frictionless operation of the protocol even during a mass slashing event.

Proposed execution plan

1. The contract has been developed, reviewed internally, and covered with the test suite PR).
2. The contract implementing the LIP is undergoing the audit by ChainSecurity, the final report will be published once finalized.
3. There will be a snapshot vote to gauge the sentiment of DAO.
4. The contract will be deployed on testnet and connected with the second opinion oracle as soon as it becomes available.
5. Mainnet voting will be covering limit change without a second opinion provider.
6. Connecting a second opinion provider to Mainnet is a question of separate discussion and voting.

Summary

Initially, it is suggested that there should be no secondary opinion source but rather an interface to integrate a preferred provider later on. Once available, the ideal secondary opinion source would be a ZKP-based Oracle, similar to those discussed on the forum (more details on this in references). Alternatively, options might be considered such as a third-party Oracle committee or even a multisig-controlled manual quasi-Oracle.

To enhance the safety of the existing design, a new strategy is suggested: instead of allowing a 5% consensus layer validator balance daily decrease, a 1.101 ETH decrease per active validator over an 18-day period is proposed (or ~3.4% consensus layer validator balance cumulative decrease over the period). This value, drawn from Ethereum specifications, addresses two out of four cases of 'Natural CLBalance decrease'—attestation penalties and the initial slashing penalty. For addressing the inactivity leak and correlated slashing penalty, which could potentially result in a loss of up to 96.88% of all Lido CLBalance in extreme cases, it is proposed to rely on a DAO vote until a trustless second opinion source is established.

References

LIP-23: Negative rebase sanity check with second opinion specification

New values calculation

Oracle V2 reporting sanity check parameter values

Oracle committee 5/9

Github repo

[ZKLLVM] Trustless ZK-proof TVL oracle

DendrETH: A trustless oracle for liquid staking protocols

ZK Lido Oracle powered by Succinct