LIP-25: Staking Router v2.0: Permissionless, secure and scalable

Abstract

Lido DAO's mission is to make Ethereum staking simple, secure, and decentralized. Recent long-range goalsapproved by the Lido DAO (and proposed by @Hasu) suggest the introduction of a decentralized validator set and permissionless staking modules.

The purpose of the thread is to summarize concerns proposed improvements to the Staking Router, in the form of a v2.0 upgrade which should be made to support permissionless modules (such as Community Staking Module) and improve security and scalability of the existing Staking Router. Should the community be generally aligned with these proposed improvements, they shall be detailed via a Lido Improvement Proposal (LIP) which will be posted in the coming weeks and put forth for a Snapshot vote.

Scope of Staking Router v2.0 upgrade

The proposed SR upgrade includes improvements to both on- and off-chain parts of the following components:

- the Deposit Security Module (DSM),
- the Validator Exit Bus Oracle (VEBO),
- the Accounting Oracle,
- and reward distribution mechanisms in curated-based modules.

Tech details can be found here LIP-25

Proposed Improvements

Deposit Security Module (DSM) improvements

Motivation

In the current implementation of the Curated modules, key vetting (the process of validating keys before making them depositable) occurs through DAO actions, and in particular EasyTrack motions, which operators may initiate after submitting keys or via full on-chain DAO votes. The proposed DSM changes aim to improve the process of key vetting to be able to work without requiring governance approval and to accommodate future permissionless modules.

Proposed Changes

1. Optimistic Vetting of Deposit Data:

Automate key vetting within DSM to enhance security and eliminate the need for governance approval.

1. Attack Mitigation:

Address cases such as incorrect signatures, duplicate keys, and front-run deposits through robust validation and reporting mechanisms.

More details: DSM Improvements

VEBO Improvements

Motivation

The current VEBO mechanism only processes validator exits in response to user withdrawal requests. This limitation hinders the protocol's ability to manage validator exits proactively, especially for permissionless modules, and thus an improvement is proposed to allow for exits for reasons other than withdrawal requests. From the Staking Router side, it is also proposed to consider a module's share when prioritizing (ordering) validators for exit.

Proposed Changes

1. Boosted Exit Requests:

Allow modules to signal VEBO to exit validators independently of withdrawal requests, using a new boosted exit mode.

1. Target Share Consideration:

Adjust validator exit prioritization to account for each module's target share, preventing disproportionate validator exits that could destabilize the module's intended share.

More details: **VEBO Improvements**

Oracle 3rd Phase Improvements

Motivation

The introduction of the Community Staking Module, which does not limit the number of node operators, necessitates a scalable solution for the Accounting Oracle's third phase report.

Proposed Changes

1. Multi-Transactional Third Phase:
2. Split the third-phase report into multiple transactions to manage large data sets efficiently and stay within Ethereum's block gas limits.
3. Ensure each transaction is processed independently but also maintains report integrity and sequence.
4. Sanity Checks and Limits:
5. Implement new gas consumption limits and sanity checks for the third phase to ensure efficient processing without exceeding gas constraints.

More details: **Expand the third phase in Oracle**

Reward Distribution in Curated-Based Modules

Motivation

Current reward distribution mechanisms, tied to the third-phase Oracle finalization hook, risk exceeding block gas limits and complicate the reporting process.

Proposed Changes

1. Decoupled Reward Distribution:
2. Implement a permissionless on-chain method to handle reward distribution independently of Oracle's third-phase report.
3. Develop a bot to trigger this method after each Accounting Report, ensuring timely reward distribution without overloading any single transaction.

More details: **Reward distribution in curated-based modules**

Conclusion

Staking Router v2.0 introduces significant improvements to Lido's permissionless staking, enhancing security and scalability.

Next steps

Stay tuned for announcements on the testnet deployments. On-chain and off-chain changes will be polished, and undergo security audits before the mainnet proposal. The final audit report will be published once finalized and on-chain vote would be proposed to upgrade the on-chain components of the protocol.

Detailed specification

Please proceed to the LIP-25 text published on GitHub for further details.

Links

- Staking Router
- Lido Oracles
- Validator Exit Bus Oracle