Merge-ready protocol service pack

Preface

As the Merge approaches, Lido dev team wants to share the plan for the Merge-ready protocol upgrade. The changes proposed are designed to be safely deployed pre-Merge.

The main change required is the ability to collect & redistributepost-Merge reward streams. At the same time, there are multiple protocol safety net improvements to be implemented along with this change, increasing the protocol resiliency & stability. Those are highly desired as the Lido has come past the 4m ETH staked threshold.

As there's a high probability of the stake surge post-Merge, the protocol should anticipate the effects it could have on the staking queue & Lido's socialized rewards distribution model.

Below we list all the changes of the "Merge-ready protocol service pack".

Changes overview

Major features

- LIP-12: On-chain mechanism for rewards distribution after the Merge

A new mechanism allowing to distribute MEV rewards and transaction priority fees acquired by validators to stETH stakers. This also introduces rewards compounding by re-staking the said rewards.

See the corresponding architecture decision record for more details.

- LIP-6: In-protocol coverage application mechanism

A coverage application mechanism provides a way for the Lido governance to burn stETH belonging to the DAO as a means of covering stETH holders' losses. It doesn't oblige the DAO to cover losses or introduce any auto-cover arrangements.

- LIP-14: Protocol safeguards. Staking rate limiting

Adding the staking rate limiting feature to have a soft moving stake amount cap per desired period.

This limit, apart from being a general safety measure, might help limit the possible staking queue growth and the resulting APR dilution in the Merge-induced market conditions (increased APR due to LIP-12).

Minor features

- LIP-7: Composite oracle beacon report receiver

A mechanism allowing to have more than one callback triggered upon every stETH rebase and receiving Lido Oracle data. The mechanism was suggested during the LIP-6 discussion and might be used within stETH L2 integrations, among other possible applications.

- [LIP-8: Increase keysOpIndex

in assignNextSigningKeys

](https://github.com/lidofinance/lido-improvement-proposals/blob/develop/LIPS/lip-8.md)

A minor change allows making NO key monitoring easier from the perspective of the off-chain services.

- LIP-9: Add an explicit log for the stETH burn events

Adds a new StETHBurnt

event emitted upon the burnShares

function invocation. The lack of this event makes writing stETH indexers and automated alerts significantly more complex. The event becomes especially relevant with implementation of LIP-6.

- LIP-10: Proxy initializations and LidoOracle upgrade

An upgrade implementing a safer and more standardized procedure for application of LidoOracle contract implementation upgrades. Doesn't change any product logic.

- LIP-11: Add a transfer shares function for stETH

Allows expressing stETH transfers in terms of rebase-agnostic underlying shares. Allows reducing precision loss in various protocol integrations.

- LIP-15: Protocol safeguards. Resume role

Allows assigning protocol emergency pause and resume privileges to different actors. This will simplify implementing a protocol emergency pause mechanism that doesn't require waiting until the full-blown DAO vote passes (72h currently), e.g. pausing by burning a significant amount of stETH or LDO (the "poison pill" mechanics).

Security considerations

Audits

We have the audit report by MixBytes team covering the whole Lido codebase with the changes above appied. The report will be published after the contracts are deployed to mainnet (since addresses are needed to finalize the audit) but before the Aragon vote for the upgrade is started.

The audit has revealed one HIGH severity issue about arbitrageability of priority fees and MEV during market spikes. The issue was fixed by implementing smoothing over the distribution of the fees (see details in the following section).

Testnets

We have tested our Merge-ready protocol setup on the Kintsugi and Kiln testnets following the#TestingTheMerge challenge.

The only missing part at the moment is MEV monitoring and tooling. That said, we believe that testing the setup with priority fees and without MEV is enough to validate the onchain part of rewards distribution since the onchain code doesn't distinguish these two types of rewards. The code is also agnostic to the particular reward accumulation flavor: whether it might be feeReceipient

setting on the validator's side or just another tail-attached transaction for the proposed block containing MEV rewards.

Limits

There are several caps and limits that were introduced as part of this upgrade to have more safeguards over the changing network and market conditions:

- Coverage application daily limit.
- MEV/tx fee daily limit.
- Staking rate limit.

Coverage application daily limit was introduced to prevent burning the amount of stETH that triggers a rebase that's sufficiently large for a front-runner to take advantage of. The possible attack was reported in the LIP-6/7-dedicated audit round.

MEV/tx fee daily limit was added to avoid similar issues when distributing a large amount of MEV or tx fees accrued between Lido oracle reports. The possible attack was reported by MixBytes.

A staking rate limit was added as a general-purpose security mechanism and also as a measure to limit possible post-Merge validator activation queue growth.

We propose to set the initial values for the listed limits as follows:

- Coverage application daily limit: 4 basis points (BP) of the total supply.
- MEV/tx fee daily limit: 1.5BP of the total supply.
- Staking rate limit: moving window of the 150k ETH per day.

The first two numbers were motivated here:Prevent large token rebases in a general determenistic way · Issue #405 · lidofinance/lido-dao · GitHub.

The staking rate limit is deduced from the historical data (daily stake varies usually from ~1k to 50k ETH per day with rare spikes up to ~200k ETH per day: 2022-03-15, 2022-05-02).

Any future change of these limits will require a DAO vote.

Action plan

Snapshot voting

A snapshot vote will be started shortly to measure the DAO sentiment towards the proposed changes.

Integrations reachout

We will reach out to the protocols integrated with Lido that might be possibly affected by the introduced changes to make sure they are prepared for this upgrade before it's applied.

Batch the upgrade into the weekly omnibus schedule

If the snapshot vote passes, the upgrade would be implemented through the Aragon votes within the "omnibus schedule" (starting on Tuesday CET afternoon and finishing on Friday). We are planning to split the upgrade into two different votings: the first one to upgrade core contracts, while having the second vote for "plugins" and "cleanups" (LIP-6, LIP-7, and minor DepositSecurityModule

fixups with respect to the audit report).

Stay tuned,

The Merge comes.