Tl;Dr

One of the parts of Lido V2 is GateSeal

(GitHub - lidofinance/gate-seals: A one-time panic button for pausable contracts):

a one-time contract that could be triggered to pause one or more contracts for a predetermined amount of time. Lido on Ethereum protocol V2 upgrade plan contains using a single GateSeal for two contracts that affect withdrawals:

1. Withdrawal queue (users' side of withdrawals).
2. Validator exit bus (Node Operators' side of withdrawals).

Initially, it's been set up with an expiration date of 1 May 2024 (Lido V2 GateSeal Committee). The proposal seeks to prolong the functioning of the GateSeal mechanics for the following year.

Context

In essence, GateSeal allows to react to the unexpected in-protocol vulnerability. In the worst case of false-positive (pause contracts if no vulnerability is present), the potential downside is limited (only withdrawals get paused, and only by limited time). In that case, leaving the protocol the option to react faster-than-governance-flow seem to be a good call. In the future, committee-driven safety mechanics could be changed to a permissionless zk-proof system. Still, that future is quite far away: it requires both the maturing of production-level zk-based tech and the ossification of withdrawals part of the Lido on Ethereum.

Proposed decision

It's proposed to use the new instance of the GateSeal Blueprint, deployed with GateSeal Factory:

- GateSeal Blueprint: 0xEe06EA501f7d9DC6F4200385A8D910182D155d3e
- GateSeal Factory: 0x6c82877cac5a7a739f16ca0a89c0a328b8764a24

The GateSeal Factory and GateSeal Blueprint contracts were audited during the V2 upgrade:GitHub - lidofinance/audits

The new instance of GateSeal will be deployed and announced under the post. The deployment verification by a third-party audit team will be posted before the on-chain voting as well.

The proposed parameters for the new GateSeal are:

- Have the same list of sealables
- Withdrawal Queue (proxy): 0x889edC2eDab5f40e902b864aD4d7AdE8E412F9B1
- Validator Exit Bus Oracle (proxy): 0x0De4Ea0184c2ad0BacA7183356Aea5B8d5Bf5c6e
- Withdrawal Queue (proxy): 0x889edC2eDab5f40e902b864aD4d7AdE8E412F9B1
- Validator Exit Bus Oracle (proxy): 0x0De4Ea0184c2ad0BacA7183356Aea5B8d5Bf5c6e
- Use the same 3/6 multisig 0x8772E3a2D86B9347A2688f9bc1808A6d8917760C in the new GateSeal: Emergency Brakes | Lido Docs
- Set the same activity duration of 1 year
- Set the same pause duration of 6 days (518400 seconds)

Next steps

If the proposal is not opposed here on the forum, the snapshot voting starts on April 11.

If the snapshot voting is approved by the DAO, the on-chain voting starts on April 23.

Stay in touch and keep your keys ready to vote!

GateSeal Committee chores

To check the liveness and readiness of the GateSeal, if the proposal is approved by the Lido DAO, it's additionally proposed to:

- Rotate at least one of the current six signers

- Hold a GateSealing drill by DAO Ops team no later than 30 June 2024

Next page for GateSeal: Dual Governance

It must be noted that the GateSeal needs to be tweaked to fit the Dual Governance design.

The proposed designed is outlined here (Dual Governance mechanism design overview - HackMD) but it could change after the internal reviews and audits.