see here for the snapshot proposal – vote expected on April 18th

[

Screenshot 2024-02-20 at 11.26.02

1562×936 184 KB

](https://europe1.discourse-cdn.com/business20/uploads/lido/original/2X/5/5b12cd4247265beb739daa56157e83797c8ed152.jpeg)

diagram taken from specification

Introduction

By allowing for stETH holders to exit en masse before a given proposal is passed, dual governance represents an important step towards mitigating Lido protocol governance risk for Ethereum stakers.

The main goal is to prevent LDO holders from changing the social contract between the protocol and stETH holders without their consent. Today LDO holders have important powers over the protocol that can result in important changes to this social contract. These include:

- Upgrading the Ethereum liquid staking protocol code.

Managing the list of the Ethereum consensus layer oracle committee members.

- Changing how the stake is distributed between node operators in a potentially harmful or unexpected way (e.g. adding or removing whitelisted Ethereum node operators).
- Changing the governance structure in an unexpected or potentially harmful way (e.g. minting or burning LDO, changing the parameters of voting systems).
- Changing the total fee percentage of the Ethereum liquid staking protocol outside of the agreed boundaries (as well as defining these boundaries).
- Deciding on how to spend the treasury

All of these powers, apart from treasury spends, directly affect stakers. Dual governance v1 allows stETH holders, in the worst case, to delay any proposed changes to the Lido protocol until they have fully exited.

V1 design

Unhappy path

Malicious proposal to change the withdrawal vault contract

1. A well-funded LDO holder makes a malicious proposal to change the stETH withdrawal contract and rug users. This proposal gets enough LDO support to pass.
2. A small group of users (stETH holders) pick up on this and vote to veto the change. In doing so they both sound the alarm for more users to join, and ensure that neither this proposal, nor any other DAO proposals (apart from treasury spends) can be executed for the time being.
3. More users join the veto while the DAO is in this temporarily frozen state (known asVetoSignalling state). Some need to take the time to unwind from their DeFi positions. That's ok.
4. The DAO remains frozen until all users that have joined the veto are able to fully withdaw their ETH (assuming the 2nd threshold has been crossed).
5. After all users have been made whole the DAO reverts back to its normal state (unless there is another veto motion already in motion).

Happy path

Good faith proposal to remove a node operator

1. For some reason or other LDO holders vote to boot a node operator out of the curated set.
2. A small group of users (stETH holders) pick up on this and vote to veto the change. In doing so they both sound the alarm for more users to join, and ensure that neither this proposal, nor any other DAO proposals which affect them can

be executed for the time being.

3. LDO holders realize they've made a mistake and de-escalate by voting to cancel all pending proposals (including the one that triggered the veto).
4. The de-escalation is successful – stETH holders remove their veto – and the DAO resumes a normal state of affairs.

Guiding objectives

The guiding objectives are as follows:

1. Give stakers a way to credibly signal their disagreement with LDO holders and the commitment to leave the protocol if LDO holders don't cooperate in resolving the incentives conflict.
2. Allow for the possibility of negotiation and de-escalation between stETH and LDO holders.
3. Introduce an extended timelock on DAO decisions that can be triggered by an active minority of stakers and prolonged as more stakers participate.
4. Improve foot voting efficiency by allowing stakers to exit the protocol without being subject to new and pending DAO decisions.
5. Don't overburden users with governance decisions

The importance of a two-phased veto with a dynamic timelock

Well-designed onchain DeFi protocols are able to put users ahead of tokenholders.

In the sense that even if the protocol is failing, users can still permissionlessly exit with their funds intact, and there's nothing tokenholders can do about it.

This is something that is truly new to financial markets and infrastructure. Something that is only made possible by the non-custodial nature of onchain DeFi.

This power of exit, is an extremely underrated differentiator between onchain Defi and offchain Defi/Tradfi.

If we want to preserve the right to exit under the most extreme scenarios, a naive Moloch style rage quit mechanism isn't quit good enough. This is because of how Ethereum's validator exit queue works – all Ethereum validator exits are processed through a single queue with limited throughput. This rate-limited exit queue means that in the worst case it could take more than a year to exit the protocol. During this time, the DAO could, in theory, pass proposals that could harm these users.

Placing a naive timelock on DAO decisions (a temporary freeze, so to speak) doesn't work either because the dynamic nature of the exit queue ensures there is no good way to place an upper limit on the length of this time.

In addition to this, many users choose to re-deploy their staked capital to other forms of economic activity, and unwinding from these positions can take weeks. If Lido only has a single veto phase, then these users would not be able exit under a worst case scenario.

In sum, a two-phase veto allows for a relatively small number of users to sound the alarm. In doing so, they can pause Lido governance proposals for long enough to either complete a negotiation and de-escalation process (happy path), or to allow for more users to join the veto and eventually exit (unhappy path). In order to avoid burdening users with politics, giving them exit guarantees is preferable to giving them full governance rights.

Committees

While dual governance needs to cover any DAO decision that can potentially affect users of the protocol, it does not cover emergency actions triggered by time-scoped circuit-breaker multisigs and contracts. There are three such committees under the v1 design.

Gate Seal committee

The Gate Seal committee is a 3/6 multisig that has the power to pause stETH to ETH withdrawals for a predetermined amount of days (currently set to 6). You can think of it as a safeguard against a withdrawal vulnerability being exploited by an attacker. The pause lasts for x days or, in the case that DAO decisions are blocked by stETH holders, until the execution of DAO decisions is unblocked. Importantly, the Gate Seal committee can only enact a pause once before losing its power (it has to be re-elected by the DAO after that). In case of non-use, the multisig automatically expires on a fixed date in the future – currently set to May 1st 2024 (see the discussion on renewing it here). At any time, the DAO can vote to appoint a new Gate Seal committee with a new expiration date.

Tiebreaker committee

The Tiebreaker committee is a more complex multisig that has the ability, under very specific conditions, to execute decisions that were proposed and approved by LDO holders but subsequently blocked by stETH holders. Note that it only obtains this right under two potentially catastrophic edge case scenarios (one in which the Gate Seal committee has paused withdrawals post veto, and another in which there's an infinite exit loop type bug). If this power didn't exist, then stETH holders who are in the middle of rage quitting could be prevented from withdrawing indefinitely.

While the GateSeal committee is optimized for speed of reaction, the Tiebreaker committee is designed for maximum security and wider ecosystem alignment: It is expected to composed of 3 or 4 sub-committees (some of which are expected to be fully-fledged DAOs). Each of these subcommittees represents a distinct interest group within the ecosystem. Any decision it makes needs to be approved by a majority (2/3 or 3/4) of sub-committees. And for each individual sub-committee to approve a decision, the latter should be supported by the supermajority of the sub-committee members. Note that no sub-committee may share members with the Gate Seal committee.

Margin of safety committee

The margin of safety committee is a temporary multisig which effectively has the power to revert Lido governance back to it's current state (i.e pre dual governance).

It exists primarily to protect from zero-day vulnerabilities in dual governance. The plan is to have a generous bug bounty to encourage responsible disclosure. It will be dissolved once this bounty program comes to an end.

Parameter choice

Clearly, getting the parameter selection right is of the upmost importance. While the mechanism design overview contains a range of possible values, finalizing these requires more research. The aim is to publish a document with suggested initial values within the next 3-6 months.

The importance of launching before 7002

As things stand today, LDO holders cannot force node operators to exit. This means that in practice, it's extremely difficult for even a captured DAO to coerce Ethereum aligned operators to do anything they would not wish to do.

EIP 7002, expected to be included in the next Ethereum hardfork (c. Q1 2025), will drastically change the balance of power here, by effectively allowing LDO holders to force exit operators. Which is why dual governance ideally needs to go live before then (or shortly afterwards).

Put another way, post triggerable exits, users need to be able to exit en masse to protect against a malicious withdrawal vault upgrade or undesirable changes to the node operator set.

How does dual governance address concerns raised by researchers?

Minimises the risk of cartel abuse

In his seminal essay on the risks of LSD, Danny Ryan writes:

Deciding "who" gets to be a NO is a matter of two questions – who is added to the set and who is removed the set. This can be designed in one of two ways in the long run – either via governance (a coin vote or other similar mechanism) or via an automated mechanism around reputation and profitability.

In the former – governance deciding NOs – the governance token (e.g. LDO) becomes a major risk to Ethereum. If the token can decide who can be a node operator in this theoretical majority-LSD, then the token holders can force cartel activities of censorship, multi-block MEV, etc, or else the NO is removed from the set.

…

Governance deciding NOs has another distinct risk which is regulatory censorship and control. If pooled stake under one LSD protocol exceeds 50%, this pooled staked gains the ability to censor blocks (and worse-so at 2/3 due to being able to finalize such blocks). In a regulatory censorship attack, we now have a distinct entity – the governance token holders – that a regulator can make requests of censorship. Depending on the token distribution, this is likely a much simpler regulatory target than the Ethereum network as a whole. And, in fact, DAO token distributions are generally pretty terrible with just a few entities deciding most votes.

Dual governance goes a long way towards addressing the above concerns. Concretely, if LDO holders tried to remove a node operator from the set unfairly, it would work as follows:

- A small quorum of stETH holders (say 2% of total) could signal their opposition to this bad decision and pause the

governance execution long enough for more holders to react. As more stETH holders join the opposition, the execution pause is extended further.

- While this is happening, LDO holders can elect to cancel the decision, and stETH holders can remove their opposition in response. If LDO holders refuse to revert course, and the number of dissatisfied stETH holders reaches a larger quorum (say 10% of total), all dissatisfied users are exited from the protocol (withdraw their ETH) and the governance execution pause is extended until this process ends.
- Importantly, governance can only be brought back to normal state if both LDO governance and participating stETH holders agree to resolve the conflict, or once all dissatisfied stETH holders have exited the protocol.

In sum, by giving stETH holders the power to impose a dynamic timelock on changes which affect them, it becomes impossible for LDO holders to force Lido protocol changes onto them. This significantly reduces the risk of capture (via cartel activities of censorship, multi-block MEV, etc).

Regarding Danny's second concern (regulatory censorship and control), stETH's token distribution is very different and much more diverse than LDO's distribution. So the combination of LDO and stETH is much more resistant to this sort of censorship. It's still not as diverse as ETH's distribution, or the distribution of Ethereum users, but this is only going to improve with time.

Ensures the right of exit under the most extreme conditions

Part of the concern today rightfully comes from the fact that stETH holders do not have full exit rights. In the sense that there exist situations in which they can be rugged by malicious LDO holders and/or node operators.

In Dankrad's words:

A very large Lido makes every decision about Ethereum staking mainly a decision about Lido, while the stETH holders are held "ransom"

By giving users full exit rights, dual governance, in combination with EIP-7002, changes this dynamic. To paraphraseVasiliy; a winning solution in open staking market can be dominant only as long as it's actually good; and what's good is ultimately decided by stakers.

Protects against insider attacks

In Vitalik's end of year 2022 post onwhat excites him, he has a wonderful section devoted to decentralized governance questions.

As he describes it, there are two big questions to answer:

[1] What kinds of governance structures make sense, and for what use cases?

[2] Does it make sense to implement those structures as a DAO, or through regular incorporation and legal contracts?

He goes on to make an interesting distinction between a governance structure and its implementation:

A particular subtlety is that the word "decentralized" is sometimes used to refer to both: a governance structure is decentralized if its decisions depend on decisions taken from a large group of participants, and an implementation of a governance structure is decentralized if it is built on a decentralized structure like a blockchain and is not dependent on any single nation-state legal system.

The framework he uses to think about this distinction is particularly powerful:

One way to think about the distinction is: decentralized governance structure protects against attackers on the inside, and a decentralized implementation protects against powerful attackers on the outside ("censorship resistance").

[

Screenshot 2024-02-12 at 16.02.48

1686×562 81.1 KB

](https://europe1.discourse-cdn.com/business20/uploads/lido/original/2X/a/a4f7d07707a3b0bb43221e6d3ab36468517849d4.jpeg)

Since liquid staking protocols, like Lido, are acting as a thin layer on top of credibly neutral global infrastructure (Ethereum), they are in the same category as stablecoins – in that they need both high protection from outside and inside attacks.

Viewed through this lens, the current structure of Lido governance is a fine model to get a protocol started, but it's not adequate for the long term. In particular, as we've highlighted above, post triggerable exits a well-funded attacker could buy

enough LDO to force exit and replace the existing node operator set with a malicious one.

Regarding innovations in decentralized governance that can protect against insider attacks, Vitalik lists two possible directions:

- Some kind of non-financialized governance, or perhaps a bicameral hybrid where decisions need to be passed not just by token holders but also by some other class of user (eg. the Optimism Citizens' House or stETH holders as in the Lido two-chamber proposal)
- Intentional friction, making it so that certain kinds of decisions can only take effect after a delay long enough that users can see that something is going wrong and escape the system.

Lido's dual governance makes important steps in both of these directions. While governance is still financialized under this first iteration, it does become a bicameral hybrid.

There is also significant intentional friction introduced by the fact that the veto is two-phased, and that veto states can be chained together. In other words, there's been alot of thought put into ensuring that users have the time to see that something is going wrong, unwind from their DeFi positions, and exit the system.

Preliminary timeline

If LDO holders approve of this direction – next week's snapshot vote (scheduled for April 18th) will serve as a temperature check – contributors plan on going forward with a technical implementation, preparing for the testnet runs, as well as engaging multiple parties to challenge the mechanism design, technical implementation, and parameter choices.

Optimistic timeline is testnet deployment in Q3, with mainnet launch scheduled for late Q3 / Q4. Note that these are approximate dates subject to change depending upon the security checks and testnet results.

Going forward

While dual governance is an important step in reducing governance risks of the protocol, it's in no way the final step.

Some ideas for v2 include:

- Allow vanilla ETH holders to trigger an extended timelock / veto
- Give some sort of veto / tiebreaker power to node operators
- Allow for delegation of stETH veto / exit power
- Allow for seamless DAO forks
- Voter bonds
- Prediction markets

Seamless forking

A promising future research direction involves looking for ways to also improve the efficiency of foot voting by node operators. For example, by allowing a subset of stakers and node operators to coordinate a protocol and DAO fork by re-pointing validator withdrawal credentials to a new contract (assuming consensus layer support).

Minimal governance

The ultimate solution to the user redemption-risk problem is governance minimization and eventual ossification of the protocol code and parameters. There's no governance risk if nothing is being governed.

Gradually minimizing the governance scope is something that Lido contributors see as a necessity in the coming years. However, until the Ethereum specification ossifies, there is only so much that can be done on this front.

In addition, any immutable code has to be formally verified on the bytecode level to minimize the risk of exploitable compiler bugs. Doing this effectively will require significant changes to the architecture of Lido's code.

Further resources

- Specification
- Mechanism design

- Research post
- Sam’s presentation
- Sacha’s presentation
- Twitter space with Hasu and Sam
- Github repo
- FAQ