- Slightly over 30% of all stake in Ethereum is staked using Lido; the share used to grow fast, but now is falling slowly.

[

Lido share graph

1100×782 115 KB

](https://europe1.discourse-cdn.com/business20/uploads/lido/original/2X/a/af1642523295dd0da5018f58f14de3d2b269f91d.png)

- Multiple Ethereans (most prominent being Superphiz, Vitalik Buterin, Danny Ryan) argue that a single staking protocol should have no more than some share amount of stake (with numbers ranging from 15% to 22% to 33%)
- This is a thread to establish all arguments pro and contra limiting Lido to some amount of stake and kick off the discussion
- The team will summarize the history of the topic.
- I would propose an extended timeline for this governance decision: three or four weeks for the discussions, then 1-week vote. We will need to establish, whether: limiting Lido is desirable; if yes, what should be the limit, what should be the mechanism and the timeline to do that. It doesn't seem like there's a need for an urgent decision and a few weeks will give the community ample time to have a say in it.
- I would ask the would-be participants of the discussion to wait a few days until we've finished on providing all the necessary context. This is a complex topic and it would benefit from having all the required nuance laid out.

UPDATE: the debate so far has been summarized by @sacha, an I'm editing in the whole thing in the first post for visibility.

# Is limiting Lido on Ethereum desirable?

Thanks to Vasiliy Shapovalov, Isidoros Passadis, Justin Drake, Tim Beiko, Ryan Berckmans, James, Joe Clapis, and Darren Langley for reading drafts of this

Ethics disclosure: This work has been funded by a LEGO grant. I do not have any direct or indirect economic interests in Lido. I do not hold any LDO, stETH, or any other staking token or associated governance token. I hold an immaterial amount of ETH.

## Motivation

Vasiliy has created a Lido forum post that frames the motivation as follows:

Multiple Ethereans (most prominent being Superphiz, Vitalik Buterin, Danny Ryan) argue that a single staking protocol should have no more than some share amount of stake (with numbers ranging from 15% to 22% to 33%.

…

[In preparation for a governance vote] We will need to establish, whether: limiting Lido is desirable; if yes, what should be the limit, what should be the mechanism and the timeline to do that.

Whether you primarily identify yourself as an Etherean, or a Lido community member, this document is an attempt to help you think through the first question – is limiting Lido desirable?

The challenge here is to provide clear and succinct answers to every question that a reasonable Lidonaut or Etherean might have, regardless of their level of education or knowledge.

If Lido is to flourish as a DAO, every LDO holder needs to be able to understand the question they are voting on, even if they are not familiar with the details of the protocol in question.

### Prominent Etherean's in favour of limiting Lido

Summary of views:

Superphiz

I wonder, who will be the first staking provider to publicly commit to limiting themselves to not operating more than 22% of validators on the chain? Who do you want to see step up to the plate and prioritize beacon chain health above profits?

Vitalik

Speculative controversial take: we should legitimize price gouging by top stake pool providers. Like, if a stake pool controls > 15%, it should be accepted and even expected

for the pool to keep increasing its fee rate until it goes back below 15%.

Danny

Lido governance controls the operator whitelist and can thus put requirements on them – e.g. exploit multi-block MEV, profitable re-orgs, or censor certain transactions

Unified profit sharing and governance levers, in the extreme, can induce the set to operate as one.

# Summary

## Why you might be in favour of limiting Lido

You might be in favour of limiting Lido if you agree with one or more of the following:

- You believe that if Lido's share is > X%, then the possibility of Lido's governance being used to coerce operators into acting as one – in order to exploit things like multi-block MEV, execute profitable re-orgs, and/or censor certain transactions – poses an existential threat to Ethereum.
- You have faith that exchanges, and other liquid staking solutions – like Alluvial – will follow suit and agree to limit themselves in the same way as Lido.
- You believe that there's a good chance even more decentralised pools, like Rocket Pool, will rise to meet the demand forfeited by Lido.
- You're sceptical that Lido holders will take the necessary steps to curtail their governance power over Ethereum over the coming months and/or that these steps – implementing proposal time locks, introducing veto rights to a quorum of stETH holders, and making parts of the protocol immutable – aren't enough to ensure Ethereum is adequately protected from a Lido governance attack.
- You believe that if stETH growth continues unchecked in the run-up to the merge, it could pose a systemic risk to Ethereum around the time of the merge (and/or when withdrawals are enabled).
- You don't believe that a winner-takes-most market is inevitable. You're of the opinion that, after the merge, competing solutions will have a better chance of gaining more share relative to Lido, but that it's important to ensure Lido's dominance doesn't become unassailable before then.

## Why you might be against limiting Lido

You might be against limiting Lido if you agree with one or more of the following:

- You believe there's a real risk an exchange-led KYC-standard would come to dominate the staking market if Lido were to self-limit, and that this would pose a greater existential threat to Ethereum than Lido governance capture.
- You trust that, during the coming months, Lido holders will take the necessary steps to curtail their potential governance power over Ethereum.
- You don't trust that exchanges, and liquid staking solutions – like Alluvial – will agree to limit themselves and commit to transparency around their infrastructure and staking flows in the same way that Lido does today.
- You don't believe that other more decentralised pools, like Rocket Pool, can scale quickly enough to meet the demand that would be forfeited by Lido.
- You believe that singling out a protocol as a detriment to the health of the network goes against Ethereum's ethos of credible neutrality.
- You share the view that the staking market is a winner-takes-most market, and hence the winner should be as good as we can make it.

# FAQ

This FAQ is an attempt to help you think through the above summary from first principles. It doesn't have to be read completely or in order. It aims to answer every question a reasonable community member might have (while assuming as little background knowledge as possible).

## What is Lido's raison-d'être?

In the core team's words:

The core reason we started Lido was to prevent a centralized exchange or group of exchanges from winning the staking market.

A key part of Lido's value proposition is liquid staking. Lido's stETH is a liquid token representative of staked ETH. When a user stakes their ETH with Lido, they are granted an stETH token. This token rebases once a day to reflect their staking rewards, and is redeemable for ETH once withdrawals on the beacon chain are supported.

Although Lido uses many independent operators, the Lido validator set is currently permissioned such that Lido takes a view as to what a good/healthy validator set backing a staking looks like. This is to prevent stETH holders from getting slashed by node operators with nothing at stake.

The other way to solve this problem is to require validators to post capital up front. This is the approach Rocket Pool takes. The upside here is that anyone can become a validator. The downside is that this approach lacks capital efficiency, which hinders growth.

### What % of total ETH staked is staked through Lido?

At time of writing, slightly over 30%. While Lido's share has more or less doubled over the last two months, it has declined slightly over the last week.

### How does Lido improve the health of the Ethereum network today?

There are 6 keys ways in which Lido improves the health of the network:

1. Legally and physically distributed validator set

Although Lido acknowledges it is currently overreliant on Europe and the U.S, it is still harder for governments to exert legal pressure on Lido than on a centralised exchange

1. Opinionated validator set

Lido actively shapes a good validator set. There are currently 20+ independent providers who adhere to high community standards and have less than 2% of the total staked ETH each (the goal is to reduce this further, Lido believes no operator should hold >1%).

1. Better client diversity

The statistics speak for themselves.

1. Non custodial nature

Instead of large amounts of stake sitting in custodial solutions, stakers control their own ETH.

1. Higher economic security

Instead of complexity and opportunity cost keeping many stakers out, stETH has unlocked the ability for far more (non-custodial) capital to secure the Beacon Chain.

1. Permissionless building block

Instead of staking confined to a walled garden, stETH is a fundamental building block for permissionless Defi.

### Where can Lido improve?

See Lido's self-assessment.

[

1155×623 117 KB

](https://europe1.discourse-cdn.com/business20/uploads/lido/original/2X/7/78c08c4a1fb316b8533941d226c4fdc657557147.png)

The main issues today have to do with governance and the validator market.

With respect to governance, there is currently no timelock between DAO vote finalization and execution

. If governance were to be captured, this could lead to a situation in which bad decisions are made before the community can intervene.

Another problem with governance today is the lack of a robust delegate set

: the delegate set is limited and, a a result, a significant amount of voting power is undelegated and dormant.

Smart contract risk is also worth mentioning here. Although multiple audits have been undertaken on all smart contract upgrades, no formal verification or symbolic execution based tests have been carried out

. The risk of a contract exploit cannot be ruled out.

## What does Lido's on-chain voting process look like today?

Lido on Ethereum is controlled by LDO token voting via an Aragon DAO. According to BlockScience's DAO vulnerability report, this includes the Lido treasury, ETH withdrawal keys, node and oracle operator lists, DAO Access Control List (ACL) permissions, the execution of EVM scripts, and more. As such, the voting app is effectively root access to Lido.

At time of writing (May 2022), the permissions on the Lido DAO are set such that:

- Any address with vested or unvested LDO tokens can create a new vote
- For a vote to pass at least 5% of all LDO tokens need to participate in the vote (approval/quorum)
- Of those who vote, 50% need to approve a proposal for it to pass (support/threshold) at the end of the voting window
- The current voting window is 3 days

## What can we learn from previous votes?

When looking at previous votes is easy to see that a small number of wallets are making most of the decisions

. Most votes are passed with close to the minimum required quorum of 5%.

## How well distributed is LDO?

The top 100 wallets control ~95% of LDO tokens

. From the Ethereum perspective, this concentration of power represents a core risk to both the protocol and the Ethereum ecosystem.

## What's the worst that could happen vis-a-vis voting?

The most worrying case is one in which an attacker makes a malicious proposal, and procures just enough LDO to swing a vote at the last minute.

The minimum number of tokens required to pass a vote is 5% of the total supply (1 billion) = 50 million LDO tokens.

Since LDO is trading at $1.12 today, the cost to procure enough tokens to pass a vote is on the order of $60M. On the other hand, stETH is close to a $10bn dollar bounty.

Note that there are plans to mitigate this concern in the short term by only allowing for votes against a proposal on the last day of a proposal. In the medium term, Lido is planning on hardening their governance by giving stETH holders and/or the operator set veto powers over proposals (however this is at least a few months away).

## Would the risks be different if Lido only used a single operator / infrastructure provider?

Even if Lido has X% of the market, that X% has the underlying work split between a group of several different independent validators / node operators.

Today, at both the key and operator layer, Lido has not tested the 1/3 threshold. However, the aggregate product has tested, and even briefly passed, the 1/3 threshold. Is this the same?

Intuitively, these cases feel different. In Degen Spartan's words:

i think the distinction must be made between numerous pool operators operating under a unified liquid staking protocol banner

vs

a single pooled staking entity having absolute control over the eth being staked with them, and has the ability to be malicious

lido is the former

On the other hand, Danny Ryan doesn't believe the distinction is all that important:

I do think that there are larger and more direct risks with a single operator, but a governance layer around a large liquid stake (>1/3, >1/2, >2/3) in the extreme can degrade to coercion of the operators acting as one

Danny's key concern here seems to be that Lido's governance layer could lead to its operators acting as one.

While Vasiliy acknowledges that this is a tail risk that needs to be addressed, he believes it is better addressed by directly focusing on curtailing Lido's governance power rather than market share:

That's much harder to exploit in practice than in theory, but it must be addressed. I just think it should be addressed by throttling the governance power of Lido (or whatever liquid staking protocol is winning) rather than throttling Lido.

## What influence can Lido's governance have over Ethereum?

The most important concern is probably the validator/operator whitelist. If Lido continues to gain market share, there's a risk that LDO holders would be able to effectively determine the majority of the Ethereum validator set.

Governance could then shepherd Lido's operators into working together to exploit multi-block MEV, execute profitable re-orgs, and/or censor certain transactions.

## How likely is a LDO governance attack on Ethereum?

If you trust the current validator set, then the main risk Lido poses for Ethereum is through the selection of a bad validator set over time. While this could happen either suddenly or gradually, it is far more likely to occur gradually.

In "The Next Chapter for Lido", Hasu explains why this is the case:

To understand why a sudden coup in Lido is impossible, one has to understand the constraints imposed by the Beacon Chain. Lido cannot yet unselect an operator after delegating to it. That means that any stake Lido has delegated thus far will not be able to change until withdrawals become available.

As a result, Lido has no significant leverage to coerce operators that are already participating to do something they don't want to do: they can't even unstake them. Even when Lido is able to rotate operators, the mechanics of the staking queue mean that it will likely take months to do so.

The second and bigger risk is for Lido to gradually worsen the validator set, especially once forced exits and withdrawals are possible. If this happens, it will likely be the result of governance capture.

Hasu's analysis breaks down however if you don't completely trust the current operator set. Once Lido is able to rotate operators, LDO holders could coerce one or several from the current set of operators to do their bidding on pain of being kicked out of the set.

## What is Lido doing to mitigate governance risk?

In order to protect against governance capture, Lido plans to rely on three measures of defense:

1. Mechanics that prevent untelegraphed changes to Lido. This will take the form of time-locks

and giving veto rights

to a quorum of stETH holders (an active area of r&d).

1. The ability for stETH holders to voluntarily unstake and move to a competitor (post merge + withdrawals).
2. The ability for Ethereum core developers to fork Lido as a last resort. From a technical PoV all it takes is to switch a few bits in the governance contract to revoke Lido's current permissions and transfer them to a community-owned contract. From a social perspective however, it's far from certain whether the entire community would choose to adopt such a fork.

## Is liquid staking on Ethereum necessarily a winner-takes-most market?

Paradigm believes the game theory around liquid staking leads to a winner-takes-most outcome. Lido's dominance on Ethereum adds weight to this hypothesis so far, but the jury's still out as to whether this is a fundamental law of PoS.

In particular it's perfectly possible that after the merge (and withdrawals have been enabled), competing solutions will have a better chance of gaining more share relative to Lido.

## What are the factors outside of Lido's control that have contributed to Lido's dominance?

While it's difficult to quantify, if the base protocol issued nonfungible validator specific staking tokens, the barrier to competition would probably be lower.

More importantly however, Lido's dominance seems to be an unavoidable consequence of making staked ETH non liquid (not withdrawable). Stakers particularly value liquidity and the ability to withdraw during a bear market. As such, the longer it takes for the merge to go live, the more likely Lido's share of the liquid staking market is to increase.

If there's one lesson for protocol designers here it's that protocols should try to ensure that the market can express itself with counter trade options. Without these, you risk the build up of systemic risk.

### Why does Lido believe it is a winner-takes-most and not a winner-takes-all market?

The thinking here is that stakers will always hold a diversity of views and values, and will therefore not allow the winning protocol to over-capture.

To quote Vasiliy:

I think this a power law market, not monopolistic (winner takes most, not winner takes all), and the leader position is hard to defend, sort of how stablecoins work.

### Does Lido dominance increase the risk of a monopoly on MEV?

This is certainly a risk worth keeping an eye on. Having said that, if liquid staking turns out to be winner-takes-most, and not winner-takes-all, then an extractive MEV monopoly is unlikely.

Block builder centralisation, which applies whether Lido exists or not, is arguably a far more real and pronounced concern from this perspective.

### Does limiting Lido run the risk of handing more power to large exchanges?

There is a good to argument to be made that, if it were not for Lido, the majority of the stake would be in the hands of exchanges (Coinbase, Kraken, Binance et al.). And a world in which exchanges – who already have ecosystem power – have private control over chain security, is strictly worse than the situation we're in today.

The question we need to ask ourselves is whether limiting Lido will lead to a larger share being captured by exchanges as opposed to other more decentralised solutions?

In particular it's not obvious whether the other decentralised pools would be able to meet the extra demand forfeited by Lido.

If a pool like Rocket Pool is able to meet this demand, then, from a dispersion of stake perspective, we would end up with a more decentralised Ethereum.

On the other hand, if RP and other decentralised version cannot scale quickly enough to meet the demand, then the most likely scenario is that exchanges eat it up.

Along these lines, Coinbase has recently announced that it is entering the liquid staking game, through its support for an institutional liquid staking protocol built by Alluvial. In Hasu's words:

I think, they plan to make the USDC of staking tokens (compliant centralized alternative to stETH)

If we were to normalise placing limits on relatively more decentralised and transparent pools like Lido, at the very least we would probably need an equally credible commitment from the likes of Alluvial and Coinbase. In particular it might make more sense to think about placing limits at the token level rather than at the staking pool level.

### What's Rocket Pool's perspective on its ability to scale enough to meet the demand that would be forfeited by Lido?

As time of writing, Rocket Pool has space for around 2500 rETH (which is around 3 days worth of new stake for Lido).

After this point, the staking pool is technically saturated and RP needs more node operators to match the collateral. However, an important counter-force here is that the node operator onboarding is growing week-on-week: minipool growth, for example, is around 140% (annualised) over the last two weeks.

For some added context, here is Rocket Pool's latest bi-weekly update:

- rETH supply has grown 1.56% to 88,107k - annualised growth of 40%
- Minipool count has grown 3.62% to 5,581 - annualised growth of 94%
- Effective RPL staked has grown 2.69% to 4.96mil - annualised growth of 70%

- Node operator count has grown 4.30% to 1,189 - annualised growth of 112%

Nevertheless, the main bottleneck today is that there are more people looking to deposit than to operate nodes – under the current design, operators must put up 16 ETH worth of collateral (not a small sum for a solo staker!).

Rocket Pool is well aware that this high collateral requirement is slowing their growth and believe they have found a way to significantly lower it without significantly increasing the rETH risk.

In parallel, the team is working on ways to support multiple parties coming together in a trust-minimised setup – so that ETH and RPL can be deposited without trusting the node operator with custody.

While neither of these improvements are expected to be ready pre-merge, they could allow RP to seriously increase its scale post-merge + withdrawals (on the order of 10-20x according to General Manager Darren Langley).

### Are the risks around non-custodial staking pools like Lido greater than the centralization risk from large exchanges?

It's hard to say. The risks are different, and it's really hard to compare them to each other. One key difference regarding exchanges though, is that the risks aren't hypothetical. The susceptibility of these entities to government pressure has already been demonstrated.

More broadly, if a KYC standard were to dominate the staking market – and become a key DeFi building block – this could become a gatekeeper problem that ends up killing the permissionless soul of Ethereum.

### Is a dynamic fee rate preferable to a hard limit?

A dynamic fee rate, as proposed by Vitalik, is probably a better option than a hard cap since remaining permissionless is important, and a dynamic limit would get around the problem of pools cementing themselves with early adopters only.

Having said that, if the limit were placed below Lido's share, then this would negatively impact current users who have no way to withdraw today.

### Is a basket of liquid staking tokens preferable to a dominant token?

Some have suggested that a meta staking token, or a basket of liquid staking tokens token would help reduce the power that any one protocol has.

While this does sound intuitively appealing, it's at least unclear whether such a token would be a net improvement.

There's a good chance that such a token would lead to an intermediary with the same power as Lido, but in a stronger position vis-a-vis fee extraction, and without the obligation to do anything useful for the protocol (for example spending time and resources curating a quality validator set or researching and developing distributed validator technology).

### Would capital seek alternatives if certain financial risks were better understood?

In Danny's words:

I'm not suggesting throttling Lido, I'm suggesting users understand the risks of pooling assets beyond 1/3, 1/2, 2/3

If the financial risks were better understood, that capital would seek alternatives

Is this an education problem at it's root?

While it's true that many leveraged stakers do not realise that they aretaking out a short position on ETH, that their position may be difficult to unwind, and that there are major penalty risks associated with co-ordinated failures of > 1/3 of the total stake, it's generally true that people tend to overlook long-term, more abstract, risks (e.g. Lido being compromised) in favour of immediate returns. This is probably not something that education can fix at a surface level.

Rather than blaming it on lack of education, it might be better for protocol designers to work under the assumption that users will almost always opt for the simpler option (or better product) when the tail risks feel abstract / hard to grasp.

### Why does Lido choose to incentivise stETH liquidity?

Lido believes that financial protocols need stETH to beliquid in order for it to be accepted as quality collateral. Once beacon chain withdrawals are enabled, stETH's liquidity is ensured by the fact that it's possible to unstake and withdraw it with a slight delay. Since this is not the case today, incentives are necessary to ensure liquidity.

### Why did Lido increase incentives recently?

Some people had overused leveraged staking to the point where as little as a 3% change in discount would have wiped

them out.

If these people had been liquidated on their positions they would have had to enter the books as forced sellers, which would have created an incentive for large players to hunt them for profit.

Lido temporarily increased the liquidity incentives on the ETH/stETH pair in order to give these leveraged stakers enough liquidity to deleverage. At the end of the day, it's LDO holders who have to pay for this.

In Vasiliy's words:

we've been open about price risks forever, loud about these risks for days, and yesterday's intervention of extra LP incentive allowed many positions to unwind a lot.

The cynical take is that this is the price Lido has to pay to avoid the negative press associated with mass liquidations.

The charitable take is a lot of folks feel they almost got burned badly and are now being more cautious. Looking at the Aave risk monitoring charts it is apparent that the amount of leverage has decreased since the incident (albeit slowly), and the amount of risky leverage present in the system today is low.

While it's true that the deleveraging of stETH/ETH is a good thing to happen significantly before the merge occurs, it remains to be seen whether a moral hazard has been created.

## Has Lido's referral program contributed to Lido's dominance?

The short answer is yes. The referral program has been responsible for around 1/4 of the ETH staked through Lido so far.

Lido pays out a lot of money in referrals (to partners such as Ledger and Argent) in order to continue increasing its market share. Previously Lido paid out 15 LDO tokens for every 1 ETH staked; today they pay 0.75% of the deposited ETH in LDO.

A snapshot vote has recently gone live to lower Ethereum Referral rewards from 0.75% to 0.50% starting in the month of June.

To quote frontalpha:

This is a continuation of Lido's efforts to gradually reduce rewards to a more sustainable level without drastically cutting rewards for partners that rely on the referral program for revenue.

## How is the stETH/ETH peg maintained?

Today, liquidity incentives (in the form of LDO emissions) are used to maintain the stETH/ETH peg. These are needed until at least the merge + withdrawals.

Once beacon chain withdrawals are enabled, stETH's liquidity will be ensured by the fact it's possible to unstake and withdraw it with a slight delay. This means incentives will no longer be strictly required.

## What happens if we have a X% depeg?

Staked positions are backed, but not redeemable until well after the merge. These positions are safe, no matter the size of the depeg, if held until redemption (assuming the merge is a success).

However, leveraged staking positions can get liquidated if the peg temporarily dislocates. You can think of this as the bounty available for temporarily moving the peg.

In short, the main concern is folks recursively borrowing ETH with stETH as collateral and staking that ETH to borrow stETH against it again (and so on). At a certain point, the ETH/stETH peg becomes very sensitive to downside risk (under some reasonable assumptions, a sustained 5% depeg could be enough to cause a series of cascading liquidations).

## How could such a depeg happen?

The stETH/ETH pool can be moved with high leverage. For example you could use Lido to stake ETH for stETH, sell stETH for ETH, and repeat until you are out of capital.

Breaking the peg doesn't look profitable today, but that could change if the leverage staking bounty were to grow relative to total liquidity in the run-up to the merge.

## Why is the merge so important for stETH?

In Tarun Chitra's words:

The premise of stETH yield is that you get:

(a) Beacon Chain yield

(b) LDO yield

While you can realise (b) immediately, (a) only really exists post merge [+ withdrawals]. Until then you can think of it as an IOU.

If people start using more leverage to multiply their expected yield from the merge this has consequences if they get liquidated right around the time withdrawals are enabled.

Post withdrawals, a liquidation cascade has the potential to dramatically reduce the % of the ETH supply staked (the signs to watch out for here are a high Lido market share combined with a high stETH average leverage ratio).

## Further Reading

- Lido Forum discussion
- Lido scorecard (self-assessed)
- "Concerning stETH liquidity" by Vasiliy Shapovalov
- "The Next Chapter for Lido" by Core Lido and Hasu
- "The Road to Trustless Ethereum Staking" by Hasu, Georgios, Konstantin, Vasiliy, Isidoros, Arjun, Jordan
- "On Staking Pools" by Georgios Konstantopoulos & Hasu
- "DAO Vulnerabilities: A Map of Lido Governance Risks & Opportunities" by BlockScience