Vibe check and anecdotal evidence from conversations with the Ethereum staking community about Lido:

[

image

1130×610 37.8 KB

](https://europe1.discourse-cdn.com/business20/uploads/lido/original/2X/a/ac0107522702cba7e3d6b8ff8c694734f8c2a92c.png)

The Ethereum community has a very healthy and passionate immune response to anything that is a threat to the decentralization and credible neutrality of Ethereum. Defending these principles was why Lido was created. Not to centralize Ethereum staking, but to provide an alternative to centralized exchange staking. This post is written by an Ethereum solo staker. It is not a post in defense of Lido, but simply a discussion about where Lido is today and what its plans are for its future.

Lido DAO contributors are working on creating permissionless modules to allow anyone to become an operator, expanding the existing permissioned set. There are two parts to that challenge, one is technical, and the other is social.

This is the first post in a series called "Lido Community Staking" that is being written for anyone who would like to learn more about the Lido protocol and DAO and what it would look like to be one of their community staking operators in the future.

About the author:

I'm Eridian, and I'm an Ethereum staking enthusiast. I wrote and maintain the EthStaker Knowledge Base and I've worked on a number of Ethereum staking-related projects such as DVStakers and Staking Directory. While participating in the Lido DVT trials, I decided to apply for the role of Community Lifeguard. The role is outlined in this forum post and the TLDR is that I don't work for Lido, I'm a community participant who is compensated via a LEGO grant for my contributions to the Lido community. All opinions are my own, I simply want to support the diversification of the Lido node operator set, enabling thousands of solo stakers to participate in validating Ethereum.

The Ethereum Staking Ecosystem today

[

image

1200×844 84.5 KB

](https://europe1.discourse-cdn.com/business20/uploads/lido/original/2X/7/7b5b9fc1330385c70e199e7c63f15cd1258211b0.png)

Source: https://dune.com/hildobby/eth2-staking

The Ethereum Staking Ecosystem without Lido

Expectation…

[

image

800×450 55.6 KB

](https://europe1.discourse-cdn.com/business20/uploads/lido/original/2X/0/0b576f92d634d0db000c5cffb1700510bfb025b1.jpeg)

Reality - A different large staking provider takes its place.

[

image

751×527 71 KB

](https://europe1.discourse-cdn.com/business20/uploads/lido/original/2X/c/c2817e18f797b22132348cd72981a60bbb635086.png)

Lido exists. While some people wish it didn't, Lido does in fact exist. It is a very significant staking protocol on Ethereum and

provides a service that people clearly want. If Lido was a bad product, or a better one was readily available, then market forces would naturally drive users toward those better alternatives. But the reality is that Lido has found a way to fill a specific need within the Ethereum staking ecosystem. Ignoring or dismissing Lido's role in the market doesn't change its significance and only leaves room for misunderstandings about the current landscape of Ethereum staking services. So, whether you're a fan or a critic, Lido's impact and continued relevance can't be overlooked.

What even is Lido?

Lido is a protocol and a DAO. A set of smart contracts deployed on Ethereum and a governance token called LDO that is used to vote on changes to those smart contracts. Operators join Lido by an on-chain transaction that is then voted on by the DAO. If they are accepted, they are assigned a number of validators. This is all publicly visible onchain. As an example, in the image below you can see that RockLogic has created 9,000 validator keys, but only 5,800 have been approved by the Lido DAO so far, and all 5,800 have been funded. HashQuark has submitted 11,000 validator keys and all 11,000 have been approved by the DAO… but only 9784 have been funded so far.

[

image

835×172 12.9 KB

](https://europe1.discourse-cdn.com/business20/uploads/lido/original/2X/8/84d7e063220403409d0cd85eccfc52cbcdcfb440.png)

Validators are funded in a round-robin where the operator with the lowest number of active validators and with available keys (in the example above that would be HashQuark) has their next validators funded.

Operators start with up to 100 approved keys which can be increased over time via a governance motion (which the Lido DAO can veto) so that operators can prove they are reliable and show they can maintain the standards expected of a Lido operator.

Could Lido force these operators to do anything? No. Lido doesn't control the validator keys as these are generated by each operator. If the protocol needs to exit a validator in order to meet withdrawal requests, all it can do is signal to the operator to trigger a voluntary withdrawal. There are updates proposed to the core Ethereum protocol that could change that in the future. For example, withdrawal address triggerable exits in EIP 7002 would allow the withdrawal address smart contract to trigger exits of validators.

Could a Lido operator change the withdrawal address of the validators they run? No. This withdrawal address is set when the validators are created and the operators never have access to the deposited ETH or the withdrawal address.

Could a Lido operator steal rewards and MEV? Yes. There's nothing technically stopping them, but there are a few things to consider when thinking about "stealing" rewards. Firstly, sending funds to the wrong address is not always malicious theft e.g. misconfiguration of clients can cause addresses to be wrongly set. For the permissioned Lido operators, the risk of theft is mitigated by aligned economic and reputation incentives. If an operator is running hundreds or thousands of validators, the risk/rewards is hugely weighted towards them following the rules. As each operator is a known entity, they also carry reputational risk from misbehaving which provides additional mitigation. If MEV stealing does occur, the DAO can vote to not allocate that operator new validators. For future permissionless operators, these incentives change, as there's no longer a reputational risk, and the reward for theft can be significantly more than the cost of the attack. Therefore, introducing permissionless operators does increase the risk of reward theft and that risk needs to be managed appropriately.

What/who is the Lido DAO, who are the largest LDO holders and what does the token distribution look like? Does LDO present an attack vector for Ethereum given Lido's significant total stake? These points are out of scope for this initial post, but will be covered in detail in the future post "LDO - Who holds the power?".

Lido is/isn't centralized?

Lido consists (at the time of writing) of 31 individual permissioned operators (with an additional 7 recently approved). They each run different hardware, different clients and can choose which MEV relays they use. They are located in diverse geographic locations and legal jurisdictions to provide high resilience and redundancy. These operators include client teams such as Prysmatic Labs (Prysm), Nethermind, Chainsafe (Lodestar), Sigma Prime (Lighthouse) and Attestant (Vouch/Dirk). You can view all the operators yourself here, here, and here.

Is Lido centralized because it only has 31 operators? What if it had 5,000+ operators and allowed for permissionless entry? Having more operators isn't a single cure to all the concerns raised about Lido. It doesn't solve the problem of the Lido DAO having indirect control over a significant portion of the Ethereum consensus layer, and more operators doesn't mean all operators are equal either. For example, if there are a few large permissioned operators with 98% of the stake and lots of smaller permissionless operators with the remaining 2%, that doesn't make it decentralized, but a highly centralized system that also has permissionless entry.

A possible scenario - A large number of permissionless operators…

[

image

1277×790 48.7 KB

](https://europe1.discourse-cdn.com/business20/uploads/lido/original/2X/1/1ddbb9bbd0a4177764b5da1db26d347210198e14.png)

… with a tiny fraction of the total validators.

[

image

1287×789 45.3 KB

](https://europe1.discourse-cdn.com/business20/uploads/lido/original/2X/4/4c78fc402c8114f05db9208aa1bf810240591ba1.png)

Even in a system where a majority of participation is permissionless, it does not necessarily make it decentralized or evenly distributed.

Lido Alternatives - Centralized exchanges

The simplest way to stake is to use a centralized exchange. It involves the minimum number of steps and doesn't require self-custody of your crypto assets. One of the main problems with this approach can be summarized with the phrase "Not your keys, not your crypto". If you have to ask permission to withdraw your assets, then one day that permission might not be granted which usually happens at times when you really need your assets back (think insolvent exchanges/bank runs). Centralized exchanges are opaque and don't rely on smart contracts to guarantee access to funds.

Lido Alternatives - Permissionless protocols

This is where Lido is moving towards with their V2 staking router and permissionless modules, but it isn't there yet. There are protocols that already allow you to join as an operator, fully permissionlessly, with no questions asked. How do they achieve this? By using a bond. A bond is a deposit that can be used to encourage good behavior and limit the influence of bad actors on the system.

Depending on how bonds are used, they can also create a capital efficiency problem. If someone with a large amount of ETH wants to stake with a protocol, a proportional amount of bond is required to match it. Even in a protocol where there was a 10:1 stake-to-bond ratio, if a staker comes along with $100m in ETH, the operators need to come up with $10m ETH in bonds just to create the validators. This limits the growth of bonded protocols forcing them to follow a narrow growth trajectory so that large amounts of ETH are not left waiting around for operators to come up with the matching bond. This is one reason why Lido has been able to scale so quickly compared to other protocols, as it can absorb almost any amount of ETH, making it very capital-efficient.

Is Lido against solo stakers?

Everyone loves a good vs. evil story. David vs. Goliath, the Rebel Alliance vs. the Empire, DeFi vs. TradFi.

Unfortunately, the reality is never that simple, and just because one option is "good" or "better" doesn't make all other options "evil" or "bad" by default. Solo staking is and always will be the gold standard of Ethereum staking. It's what the protocol has been designed for and is the measure by which all other staking solutions should be compared.

However, not everyone can run their own Ethereum staking machine. There are many reasons for this including the capital cost of the required ETH and the desire to set up and maintain hardware. These are not insurmountable issues and there are entire communities such as EthStaker who make it as easy as possible to solo stake. However, even with all of these resources available, there are many people who will not solo stake from home and instead look to a service provider.

Lido Community Staking

If you want to stake on Ethereum today, there are a number of options available to you:

- Solo stake (requires 32 ETH)

- Buy an LST (e.g. rETH, stETH)

- Stake with a pool (e.g. Stakefish, p2p)

- Operate a node with a pool (e.g. RocketPool, StakeWise V3, Stader, Diva)

(Check out staking.directory for a list of available Ethereum staking options

)

This list is set to grow quickly with many new staking pools and DVT solutions coming to mainnet soon. You could apply to be a permissioned Lido operator, but this requires a proven track record of staking, professional infrastructure, incident response teams, etc., so it's challenging and very competitive!

As a result of the Lido V2 update, modules can be created that allow for a wider range of staking parameters, with a permissionless solo staking module being a top priority for many Lido DAO contributors.

While the details are still being worked out, the idea is that anyone (permissionlessly!) will be able to become a Lido node operator and run an Ethereum validator. There will likely be a bond requirement for security and economic alignment, but that bond will be significantly less than the 32 ETH required to solo stake.

A detailed description of V2 modules will be explained in a future post "Lido V2 modules explained for Solo Stakers".

So, is Lido good for Ethereum?

Ultimately, Lido fills a specific role within the Ethereum staking landscape. This post wasn't written to give a direct answer to that question, but instead to provide information to show what Lido looks like today and its direction in the near future. Lidos value to Ethereum depends on how it adapts to challenges and critiques concerning its governance and decentralization. As the Ethereum staking ecosystem continues to evolve, keeping a balanced perspective on protocols like Lido is necessary for a resilient, inclusive, and decentralized network.