On December 1st, 2020, Ethereum began its transition to proof of stake (PoS) by launching the Beacon Chain. While this allowed users to stake their ETH for the first time, there were still several points of friction:

1. No unstaking:

Once deposited, stakers cannot withdraw their stake until transfers from the Beacon Chain are enabled. This makes staking a one-way road for many months, if not years, to come.

1. Illiquidity:

While staking, users cannot move, trade, or use their ETH as collateral in DeFi. This is especially costly as long as they cannot withdraw from the Beacon Chain.

1. High capital requirement:

Users can only stake in multiples of 32 ETH, excluding users with smaller or uneven balances.

1. Operational burden:

Although Ethereum core developers made sure that staking has low hardware and uptime requirements, many users prefer to provide the capital and outsource the operational work to a third party.

It has long been clear to us that users would want a solution to these problems, and we wouldn't be the only ones trying to provide it.

The first, and most obvious, contender were centralized exchanges. For them, it would be trivial to pool the ETH of their users (solving #3

), stake it for them (solving #4

), and issue a liquid token that represents their locked stake (solving #1-2

). Given how valuable customer acquisition and liquidity are to exchange businesses, they can even offer this service at no additional cost to the user.

Fast forward to today, and centralized exchanges are emerging as the early winners of Ethereum staking. Publicly known validators operated by exchanges like Kraken or Binance are among the largest stakers. Less visible exchanges like Coinbase could make up an even larger share of staked ETH.

Breakdown of Ethereum staking services:

[

1141×1600 209 KB

](https://europe1.discourse-cdn.com/business20/uploads/lido/original/1X/b115e0bd3bc82d0abf9e6809004f0e508540c5d7.png)

However, exchanges are already among the most significant users of Ethereum; making them the largest block producers could significantly harm Ethereum's decentralization.

For that reason, we believe decentralized staking pools like Lido

are required to provide a competitive alternative to centralized exchange staking.

Why is it so crucial that an Ethereum staking pool is completely trustless?

1. Central to Ethereum's security:

As discussed earlier, many users will want to delegate their stake. But since Ethereum does not support in-protocol delegation, it leaves a vacuum for third-party providers to fill. Given how central staking is to Ethereum's security, a trustless pool is strongly preferable to a trusted or centralized one.

1. Staking has centralizing forces:

The staking landscape may be more centralized than the mining landscape, supporting fewer, more concentrated winners. That is because a staking pool's ability to issue a liquid staking token like stETH creates a powerful network effect that doesn't exist in proof of work mining.

In this post, we want to explain the thoughts that led to Lido's current design and how we plan on transitioning Lido to a piece of fully trustless infrastructure.

Creating a trustless staking pool and token

When we launched Lido, it was not possible to create a fully trustless staking pool and token. So we had to choose between a) delaying our launch or b) providing the best possible alternative to exchange staking while minimizing the amount of trust required.

Though the second approach required more trust from users, waiting would have ceded the playing field to exchanges who don't impose the same restrictions on themselves. It's not clear if trustless staking could have overcome such a big first-mover advantage, making waiting seem like the riskier option to us.

As a result, we chose an iterative approach, allowing us to compete with exchange staking and capture market share while continually reducing trust in the system as the possibilities for doing so become available.

So, what are the key factors preventing a fully trustless staking product today? Right now, we can identify three main points where users need to trust Lido:

1. Deposits made before July 15th, 2021 are not non-custodial:

When we launched Lido, it was impossible to set a smart contract as the owner of a beacon chain validator. So the withdrawal credentials of the Lido validators are controlled by a 6-of-11 multisig of reputable Ethereum builders. We have since transitioned custody to a smart contract, but this cannot extend to existing deposits yet.

1. Withdrawals are currently not permissionless

: Because of how withdrawal credentials are designed, Lido validators currently have to unstake manually. As a result, stETH holders cannot force Lido node operators to unstake and must instead trust them to act honestly and not grief.

1. Becoming a node operator is currently not permissionless:

Only the Lido registry, which LDO token holders control, can add new node operators today. As a result, stETH users trust that LDO holders will continue to uphold a sensible and well-distributed validator set.

Note that withdrawals from the beacon chain are not yet enabled, so nobody—including the 6-of-11 multisig—can withdraw funds from the deposit contract anyway. That also means an stETH holder can currently not claim ETH from the beacon chain, and hence they cannot be griefed. As a result, the first two issues are not exploitable today. But we do include them because they would become issues the moment withdrawals are enabled.

Removing these trust requirements

Transitioning custody to a smart contract

As discussed before, it was not possible to set a smart contract as the owner of a beacon chain validator when Lido launched. The smart contract withdrawal address format has since been added to the beacon chain spec, and last week we switched the withdrawal credentials of new depositors to a smart contract

To understand why this cannot apply to existing deposits, we need to take a quick detour to understand withdrawal credentials in the beacon chain:

1. As described before, Ethereum staking started with only one type of withdrawal credential, called 0x0. This allowed only a BLS address type to be the owner of a validator, not even an Ethereum address.

2. In December 2020, the introduction of 0x01 allowed Ethereum addresses to own a validator.

3. To switch the withdrawal credentials of an existing validator, one would have to unstake the ETH and then restake it with the new credentials. However, unstaked ETH cannot be restaked until withdrawals are enabled. So to switch from 0x0 to 0x01 today, a second mechanism is required, which would allow validators to switch their withdrawal credentials "in-flight."

The smart contract we use for new withdrawals is implemented as a skeleton upgradeable smart contract. This is done because we are still missing critical functionality for implementing remote withdrawals

(i.e., a smart contract triggers a validator to unstake), so we need the option to upgrade when these are introduced.

The upgrade to smart contract withdrawal credentials happened on July 15, 2021. Any new deposits made after that are fully non-custodial.

Forcing a validator to unstake remotely

If a user wanted to unstake today (which doesn't make sense since the ETH can neither be withdrawn nor restaked), Lido would have to issue a message to the validator. That validator then has to unstake manually, allowing them to grief or even

extort Lido. To mitigate this, we have been onboarding new node operators in a permissioned manner so far.

Optimally, we would completely solve the problem by allowing stETH holders to trigger a withdrawal from the beacon chain remotely

. Recently, Ethereum researchers have made a[new proposal](#) that would enable the delegator to force their delegate to unstake. Temporarily labeled 0x03, this could be either implemented as an independent credential or as an amendment to 0x01 once beacon chain withdrawals become enabled.

The proposal works by introducing a new “canonical” Exit Contract on Ethereum (like the Deposit contract). The 0x03 withdrawal credentials owner would specify any validator with the matching withdrawal credentials. Then the Beacon Chain would trigger a “[voluntary exit](#)” for that validator as part of the beacon chain state transition function. This means that the validator is remotely unstaked.

Opening up the registry

As we saw, the custody and griefing attack vector have straightforward technical solutions. Fortunately, they are also the most important problems, and solving them are the top two priorities for making Lido more trustless for stakers.

That leaves us with the question of who is allowed to be a node operator for Lido. This is a more complex problem, where the solution space is not nearly as straightforward.

First, why does Lido need to control who can be a node operator?

A core part of Lido’s value proposition is liquid staking

, so the issuance of the stETH token against a user’s deposit. In a naive implementation, tokens issued against different validators should trade at different market prices because they vary in performance and reliability. However, the resulting tokens wouldn’t be fungible against each other, making it much harder to build liquidity for them.

Instead, Lido users get issued the same fungible stETH token from their deposit, allowing exchanges, lending markets, etc., to adopt it.

This fungibility, while highly desirable, creates a new problem of its own: it requires us to socialize the performance and slashing-risk of bad validators across all stETH holders

instead of just the holder of the individual validator’s token. For example, if one validator gets slashed, all stETH holders lose a little bit of performance, instead of one token holder losing a lot.

In a world with non-fungible staking tokens, users would have to incentive to stake with the best node operators because their quality would reflect directly in the value of their staking token. In other words, the market would perform quality control on who gets to stake

. But in a world where the token is fungible, Lido has to ensure that only qualified stakers receive delegation

.

This central “quality control” of stakers is a non-trivial problem. We present a non-exhaustive list of possible solutions:

Central registry + off-chain reputation

: The simplest solution is to allow only top node operators with a proven track record and legal recourse, who can be voted in by LDO governance. This describes the current solution, but it may give governance too much power over Ethereum. This would be the case if the network effect of stETH got so strong that people use it even if a different provider would be better for Ethereum’s decentralization.

Staker-curated registries:

A more decentralized and value-aligned solution would be to make stakers choose the sets of node operators. That is a non-trivial problem, as the stake is liquid, and, by definition, stakers don’t have to live with the long-term consequences of their actions. However, if solved, it would allow for a permissionless protocol strongly aligned with stakers’ interests.

Bonding

: One approach other blockchains like Tezos and other staking pools like Rocket Pool use requires a bond from validators. For example, in Rocket Pool, validators have to stake alongside their delegator. In a 1-to-1 bonded system, there’s effectively no slashing risk for the customer because the system would also slash the validator’s bond first.

However, as we have seen many times across crypto history, capital efficiency matters a lot, and bonded solutions often come to market later, scale more poorly, and are more expensive for holders than unbonded ones. It stands to reason that the same dynamics will apply to the staking market. Even worse, they give a considerable advantage to custodial liquid staking solutions (e.g., exchanges) that can freely use other people’s tokens for bonding.

Secret Shared Validators:

One way to increase the system's fault tolerance without hurting its performance is via a new proposal pioneered by the Ethereum Foundation, called Secret Shared Validators (SSV).

An SSV splits an individual validator into a multisig controlled by different entities. These entities would then produce blocks together by first coming to consensus via an off-chain voting protocol. While coming at the cost of higher communication overhead, a single validator could no longer cause any faults on their own because instead of controlling one validator, they might control 10% of 10 validators.

A strategic commitment to researching SSVs is currently discussed in the Lido forum.

Tracking validator performance

: Another low-hanging fruit could be to track the in-protocol performance of validators and use that information to allocate ETH inside the system. As a first step, the beacon chain would need to expose validator statistics (e.g., uptime) so that the staking pool smart contract can calculate the performance on-chain.

This could be used in several ways. For example, node operators with better performance could have a higher chance of getting allocated new ETH that comes into the system than worse validators. Further, when somebody wants to unstake their ETH, the system could remove the worst-performing validators instead of a random one.

Insurance:

Lido could again outsource the quality control over validators to the market, e.g., by having a public insurance system. This would effectively be a prediction market where Lido pays rewards for predicting what validators will have the best monthly performance.

Node operator score

: To reiterate, Lido needs to impose quality control on who gets to be a node operator. Still, it wants to do it in a way that requires no centralized control from LDO governors or anyone else.

The optimal solution could combine many of the above ideas into one validator scoring system. Whenever new ETH is queued for staking, higher-scoring node operators would have a higher chance of receiving the ETH than lower-scoring ones, up to a safe limit. Low scoring node operators could also be punished first when ETH is withdrawn, or even be removed from the system entirely if they fall below a minimum threshold.

Every new node operator coming into the system could start with a 0 score, implying low trust and a small chance to receive delegation. Node operators could then collect points by performing various trust-inducing actions, such as:

- being part of a many-person SSV.
- bonding some of their own ETH.
- having insurance staked on them.
- and primarily, showing a good validator performance over time.

(These are only some indicative ways to score a node operator. More/better options may exist.)

Anyone can become a node operator in a system like that, but they would have to display similar qualities as they would have in a market where users choose their delegate. As a node operator builds a good track record over time, they could reduce other costs like insurance or SSV overhead. It would also create an incentive to perform as well as possible because it leads to being rewarded with more stake.

Whatever the optimal solution is, Lido is committed to finding and implementing it to the best of our abilities.

Summary

We believe the winning Ethereum staking pool and token will be a maximally decentralized and immutable protocol, and this is the optimal end state for Lido.

We also believe that waiting for Ethereum to be 100% compatible with such solutions will effectively forfeit the market to centralized actors who don't impose similar constraints on themselves. As a result, the best path to provide a trustless alternative is through iterative change that adopts the best possible practice at the time.

We are on track to making Lido fully non-custodial and trustless for stETH holders. Our two top priorities have clear technical solutions that we're working on with Ethereum developers or waiting to deploy when it's possible to do so.

Trustless entry for node operators is a more complicated problem to solve. Still, we will explore the solutions above as well

as others we haven’t thought about to reduce Lido’s reliance on governance as much as possible.

We’re committed to continuing to iterate quickly and reduce trust surfaces required in the Lido system as solutions become viable. We’re proud to have offered a better alternative to centralized exchange staking and led the way to build fully decentralized, trustless staking token.

Signed:

[Hasu

](https://twitter.com/hasufl) ,

[Georgios

](https://twitter.com/gakonst) ,

[Konstantin

](https://twitter.com/Lomashuk) ,

[Vasiliy

](https://twitter.com/_vshapovalov) ,

[Isidoros

](https://twitter.com/IsdrsP) ,

[Arjun

](https://twitter.com/arjunblj) ,

[Jordan

](https://twitter.com/cryptocobain)