Lido: Ethereum Liquid Staking

Abstract. Lido DAO is a community that builds liquid staking service for Ethereum. Lido allows users to earn staking rewards without locking assets or maintaining staking infrastructure. Staking with Lido is primed to start along with Phase 0 of Ethereum 2.0.

Ethereum is soon to be the biggest staking economy in the space. However, staking on the first stages of Ethereum 2.0 comes with a high market risk related to frozen staked assets until transfers will be available in Ethereum 2.0 (Phase 1.5 or Phase 2), which is expected to happen next year at the earliest. Until that time, no one will be able to withdraw staked ether, and, for example, sell them on an exchange.

Lido liquid staking protocol is an Ethereum 2.0 liquid staking protocol solving these drawbacks. Users can deposit their ether in Lido smart contracts and receive stETH -- a tokenized version of staked ether -- in return. The DAO-controlled smart contracts then stake tokens with DAO-picked node operators. Users' deposited funds are controlled by the DAO, node operators never have direct access to the users' assets.

Unlike staked ether, the stETH token is free from the limitations associated with a lack of liquidity and can be transferred at any time. The stETH token balance will be calculated based on the total amount of staked ether, plus rewards and minus any slashing penalties.

Lido is a much more flexible solution than self-staking since it avoids freezing assets and maintaining a validator node. In addition, it allows staking users to earn rewards on as small a deposit as they want without restriction on the number of ether deposited.

At the start, the system applies a 10% fee (this can be changed by the DAO) on staking rewards that are split between node operators, the DAO, and a slashing insurance fund. This fee level should make Lido staking more profitable than what is offered with most available exchange staking, but, unlike them, Lido's amount of staked ether is fully auditable and does not rely on a single party's private key management. Despite the strict limitations of the beacon chain, the first stage of Ethereum 2.0, we propose a decentralized approach for liquid staking.

1. Ethereum 2.0 staking summary

Ethereum 2.0 is undergoing heavy research and development and is going to bring innovation, including the transition to a proof-of-stake based consensus algorithm. The process of staking involves locking up an amount of ether in a wallet to participate in the blockchain consensus in return for rewards. A lot of users are showing interest in staking, which will allow them to generate income.

However, the transition to Ethereum 2.0 is planned to occur gradually. Staking will be available from the very beginning (deposits are already enabled and the network itself will launch, most likely, in December), but the coins that the user deposits cannot be withdrawn until transfers are enabled. Full support for withdrawal mechanics will not appear until Phase 2 or Phase 1.5, which is scheduled to roll out over the next few years.

Ethereum 2.0 launch will involve 4 stages (release dates provided by ConsenSys):

- **Phase 0:** the main beacon chain without shards will be implemented - chain validators create blocks according to the PoS algorithm. Transactions are not supported and, in particular, there are no fund transfers, i.e. the chain consists only of service data.
  Release date: 1 December 2020.
- **Phase 1:** 64 shards will be added. There is still no transaction support (i.e., all shards contain only service data). *Release date: 2021.*
- **Phase 1.5:** the current Ethereum network becomes one of the shards. *Release date: 2021.*
- **Phase 2:** ether accounts, transactions, transfers, and withdrawals will be added. There are no clearly defined specifications yet. *Release date: 2021 or later.*

To validate the beacon chain, a user needs to deposit 32 ether, specify a validating public key, and a withdrawal address where their assets and rewards will stay frozen until transfers are enabled. Until then, the only two activities performed on the beacon chain are validating and to stop validating. To participate in the network consensus, a validator must maintain high uptime.

There is a risk of loss or loss of profits, which occurs if the validator is slashed for misbehaving. This can happen, for example, due to a bug in the validator's node code or due to connectivity issues.

Taking into account all the details and risks, ether staking becomes less attractive in the early stages. The main issue is locking the staked deposit for a long time without the ability to withdraw.

Exchange staking is a custodial alternative to self-staking, as users can earn rewards with the ability to withdraw their coins at any time. Exchanges can instantly return coins on demand from the liquidity pool without waiting until the end of the unbonding period. Exchanges apply a fee on profits from a staking deposit.

Exchange staking for Ethereum 2.0 is additionally complicated by a lack of ability to withdraw staked coins in the first stages. Therefore, an exchange could safely stake only a share of deposits, up to 60% of the deposited ether in our estimations, to ensure liquidity to allow users to withdraw their staked funds. As a result, the Ethereum 2.0 exchange liquid staking interest rate will be significantly less than self-staking.

2. Goals

Lido aims to allow users to stake ether without losing the ability to trade or otherwise use their tokens. Lido will be a decentralized infrastructure for issuing a liquid token that is safer than exchange staking and has incredible flexibility compared to self-staking.

The primary goals of Lido are:

- To allow users to earn staking rewards without fully locking their ether;
- To make it possible to earn rewards on as small a deposit as users want without restriction on deposits different than 32 ether;
- To reduce the risks of losing a staked deposit due to software failures or malicious third-parties;
- To provide the stETH token as a building block for other applications and protocols (e.g., as collateral in lending or other trading DeFi solutions);
- To provide an alternative to exchange staking, self-staking, and other semi-custodial and decentralized protocols.

3. Why DAO

The Lido DAO is a Decentralized Autonomous Organization, which builds liquid staking protocol for Ethereum.

In the case of liquid staking, the competitors are well-known providers like centralized exchanges and other decentralized protocols like RocketPool. The DAO is the logical compromise between full centralization and decentralization, which allows the deployment of competitive products without full centralization and custody on the exchanges.

We do not believe that it is possible to make a liquid staking protocol that is completely trustless. For the first phases of Ethereum 2.0, it is not possible at all.

A DAO is an optimal structure for launching Lido because:

- Lido is highly dependent on the design and restrictions of the beacon chain;
- Ethereum 2.0 staking protocol may change and therefore Lido should be upgradable;
- An insurance provider must be selected and terms for slashing insurance must be negotiated;
- DAO governance is better than one person or a developer's team for making decisions about changes in Lido; and
- a DAO will be able to cover the costs of developing and upgrading the protocol from the DAO token treasury.

The DAO will accumulate service fees from Lido, which can be funneled into the insurance and development funds, distributed by the DAO.

4. System Architecture

Lido is managed by the Lido DAO. The DAO members govern Lido to ensure its efficiency and stability. Besides technical development, the Lido DAO's mandate is to promote Lido and recruit new users, node operators, and validators with educational content, promotional campaigns, and affiliate marketing.

The Lido DAO should do the following:

- Launch Lido:
  - Deploy protocol smart contracts;
  - Set fees and other protocol parameters;
  - Select the threshold signature scheme participants among reputable individuals or organizations willing to provide the service;
  - Facilitate the multi-party computation ceremony to create the threshold signature account for staking rewards;
  - Assign initial DAO-vetted node operators.
- Propose and update Lido's parameters;
- Approve incentives for parties that contribute towards DAO's goals (e.g., stETH liquidity providers);
- Propose and update Lido's implementation for incoming Ethereum 2.0 features using DAO treasury funds;
- Assign oracles to deliver reward/slashing rate feed to help establish stETH token balances;
- Scout and qualify new node operators and penalize the existing ones slashed by Ethereum 2.0's rules;
- Manage the Lido DAO's insurance and development funds;
- Manage unbonding and withdrawals once available in Ethereum 2.0; and
- Respond to emergencies.

Lido is implemented in a trust-minimized way as a set of Ethereum 1.0 smart contracts. Lido allows users to earn staking rewards on their ether holdings, without locking capital or maintaining the validator's node.

Lido consists of several parts:

- stETH Token;
- Deposits and stETH token minting;
- Node operator registry;
- Beacon chain oracles and stETH token balance update; and
- Withdrawals (disabled until Ethereum 2.0 transfers are available).

To stake ether with Lido, the user sends ether to the smart contract and gets stETH tokens in return. stETH tokens represent a tokenized staking deposit. stETH tokens can be held, traded, or sold. The balance of stETH is based on the total amount of staked ether plus total staking rewards and minus slashing applied on validators.

All deposits into Lido are delineated by 32 ETH and assigned to node operators who validates using these deposits. Node operators never have direct access to the users' ether.

Funds are deposited to the Lido protocol smart contract and then are locked into the Ethereum proof-of-stake deposit contract. The threshold signature account controlled by the Lido DAO is specified as a staking withdrawal address. Staked ether will be withdrawable only when transfers and smart contracts will be implemented on Ethereum 2.0 (expected in Phase 2).

Unlike similar systems, Lido does not require node operators to deposit equal collateral of staking positions. Instead, Lido DAO-chosen node operators should have a track record with assets staking, which will be supplemented with slashing insurance. This approach will allow the system to be more capital-efficient.

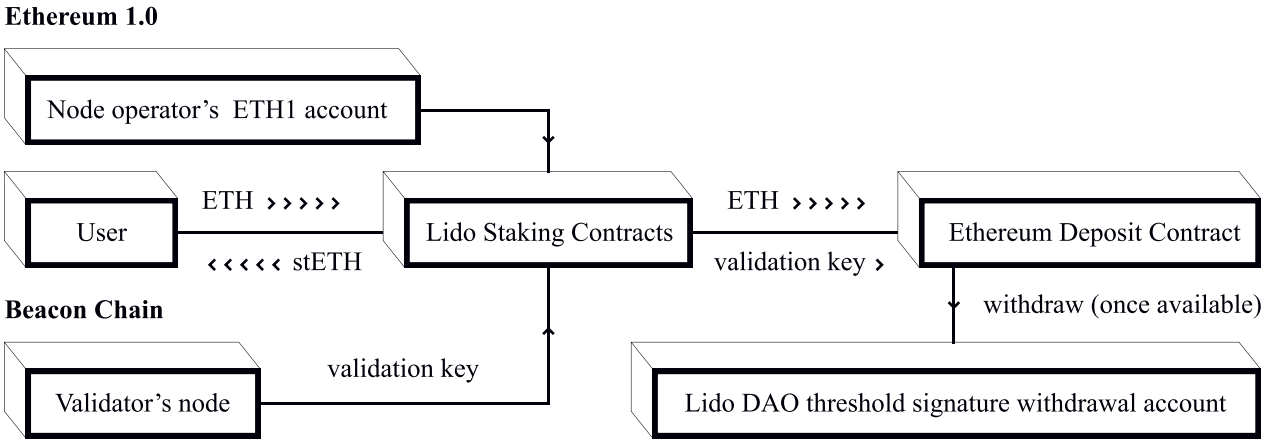

Figure 1: Stake Deposit Flow

The stETH token balance is based on the amount of ether deposited in Lido with associated total rewards and slashing penalties. Since the beacon chain is a separate network, Lido smart contracts cannot get direct access to its data. Communication between the Ethereum 1.0 part of the system and the beacon network is performed by the Lido DAO appointed oracles. They monitor node operators' beacon chain accounts and submit corresponding data to Lido's Ethereum 1.0 smart contracts.

On every update submitted by oracle, the system recalculates the stETH token ratio. If the overall staking rewards are greater than the slashing penalties, the system registers a profit. In this case, the stETH token balances will increase and Lido would apply a 10% fee.

The fee is applied by minting stETH tokens corresponding to 10% of Lido's profit. The minted stETH tokens are distributed between the node operators and the DAO's treasury account. Node operators' part of the fee is distributed proportionally to the corresponding active validation keys on the beacon chain.

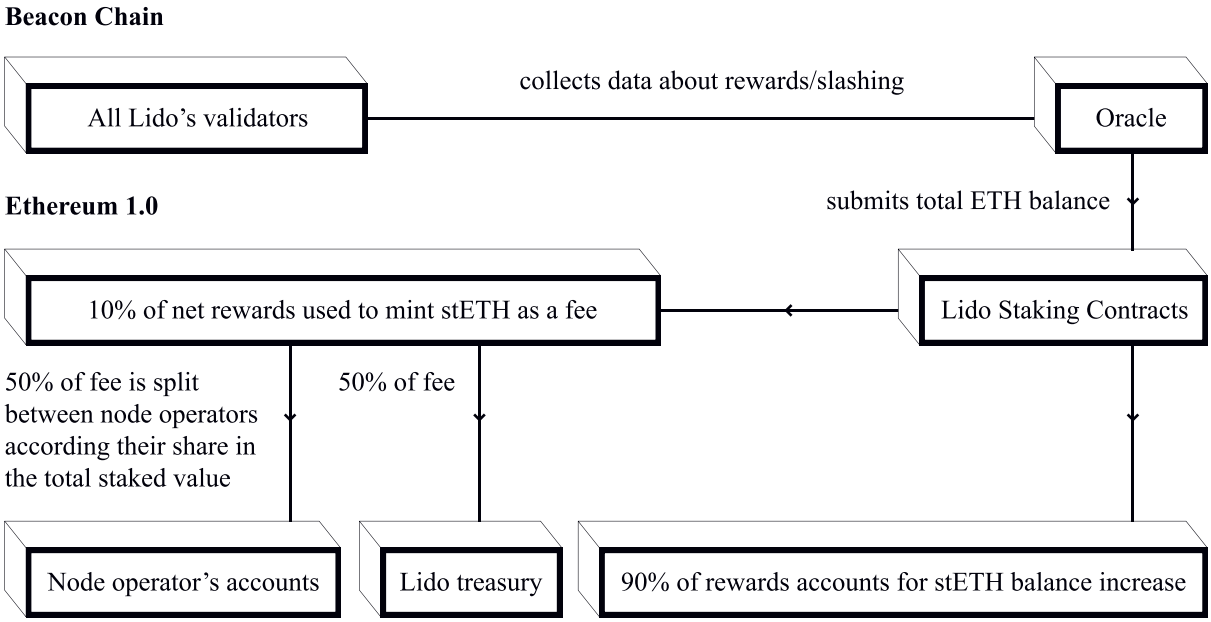

Figure 2: Staking profit distribution

Slashing penalties negatively impact stETH token balances. To compensate for this negative impact, part of the Lido fee is transferred to the slashing insurance provider who protects against reasonably-sized slashing events. The Lido DAO governance must intervene in case of massive slashings.

Withdrawals will be available once transfers are implemented in Ethereum 2.0 (scheduled as Phase 2). Once Ethereum 2.0 transfers are rolled out, the Lido DAO would upgrade Lido to implement the feature. Before that point, rewards restaking is not available either.

5. Tokenomics

Lido has two tokens: liquid stETH token — a tokenized version of staked ethereum — and LDO — a token granting governance rights in the Lido DAO.

5.1 stETH token

The stETH token is a tokenized version of staked ether. When a user sends ether into the Lido liquid staking smart contract, the user receives the corresponding amount of stETH tokens. The stETH token represents Lido user's deposits and the corresponding staking rewards and slashing penalties. The stETH token is a liquid alternative for the staked ether: it could be transferred, traded, or used in DeFi applications.

Lido makes the stETH token balance track a balance of corresponding balance of beacon chain ether. A user's balance of stETH tokens corresponds 1 to 1 to an amount of ether a user could receive if withdrawals were enabled and instant.

Ethereum 2.0 transfers and smart contracts are scheduled at Phase 2. Once these features are deployed, the Lido DAO will upgrade Lido to allow the users to burn stETH tokens in exchange for ether.

While the fact that a stETH balance tracks the corresponding amount of beacon chain such that ether should be the main driver of the stETH/ETH exchange rate, several other factors are affecting the market prices.

There is a market risk that the stETH token supply will outweigh the market demand. While the goal of the Lido is to provide liquidity for ether staked on the beacon chain, the same liquidity makes it possible to sell the token on exchanges. Before Phase 2 deployment, it is the only way to take profit from the stETH token.

However, stETH tokens also can be used in various decentralized financial products. For instance, stETH could be used as collateral. The higher the rate of stETH adoption in different DeFi applications, the more demand for it there would be.

5.2 LDO token

Lido DAO governs a set of liquid staking protocols with Lido on Ethereum among them. The Lido DAO decides on Lido's key parameters (e.g., fees) and executes Lido upgrades. The Lido DAO members govern Lido to ensure its efficiency and stability.

To have a vote in the Lido DAO, one must hold its governance token, LDO. LDO voting weight is proportional to the amount of LDO a voter stakes in the voting contract. The more LDO locked in a user's voting contract, the greater the decision-making power the voter gets. The exact mechanism of LDO voting can be upgraded just like the other DAO applications.

6. Risks

6.1 Smart contract security

The security of Lido must be the Lido DAO's highest priority beginning at the time of its deployment. Users should investigate risks involved with Lido before engaging with it. There is an inherent risk that Lido could contain vulnerabilities or bugs causing, among other things, the complete failure of Lido and/or its parts.

6.2 Beacon chain technical risk

Lido on Ethereum is built on top of experimental technology under active development. There is no guarantee that the beacon chain network would be error-free or have a minimum uptime. Failures in Ethereum 2.0 might lead to validators slashing and result in a significant drop in the balance and price of the stETH token.

6.3 Beacon chain adoption risk

The beacon chain's staking rewards are the source of the value increase of the stETH token. In case the beacon chain network does not reach its target adoption, the value of the staked beacon chain ether and the staking rewards could be significantly lower than Ethereum 1.0 ether.

6.4 DAO threshold key management risk

All Lido DAO staked ether is held on distributedly managed accounts backed by a BLS based m-of-n threshold scheme. The threshold scheme is more secure than a single key controlled by the custody. However, there is still a non-zero probability of failure. If at least (n-m+1) signatories lose their key shares, get hacked, or go rogue, funds might become locked. If m or more key shares are compromised, funds can be stolen (after transfers are unlocked).

6.5 Slashing risk

Beacon chain validators are at risk of receiving staking penalties (for going offline, for example) and slashing (for double signing). In the worst case, when a lot of validators misconduct simultaneously, up to 100% of the stake can be slashed. To mitigate this risk, the stake is distributed to a plethora of professional and reputable node operators with heterogeneous setups. Additional mitigation comes in form of insurance that is continuously paid for from Lido fees.

6.6 stETH price risk

Besides the risk associated with validators' slashing and a stETH token balance drop, there is a chance that the exchange price of stETH will be less than fair price for a while. In the beginning, there is no withdrawal feature in Lido. As a result, arbitrage and risk-free market-making are impossible.

7. Conclusion

We are in the middle of a big Ethereum transition from the proof of work to the proof of stake consensus model. Security of the network depends on the amount of the total staked ether and the level of validators' decentralization — how many the network would have and how big they would be.

As withdrawals are not available on the beacon chain, there is a risk that some users would not be able to afford self-staking. Because of that, users would either use some sort of exchange staking or pass on the staking altogether.

Limitations of the beacon chain affect the liquidity of staked capital for exchanges. We expect that most exchanges would not be able to offer rewards comparable to self-staking. The other thing to look out for is the high risk of network centralization. Exchanges are historically among the biggest ether holders, and they could become even bigger due to exchange staking.

Liquid staking provides a viable alternative to both self and exchange staking. Lido provides a balance of risk, reward, and convenience. It allows users to trade staked ether without a negative impact on the Ethereum network's decentralized nature.

Lido is useful for both small and large ether holders. Small wallets could use staking without having to stake big chunks of their funds. Larger entities would be able to hedge their funds against ether volatility and use staking without having to maintain staking infrastructure.