Hello everyone! We're Hyperelliptic Labs and RockX, and to continue the monumental success of the LEGO Initiative, we propose an expansion of the family of Lido liquid staking protocols into Avalanche. We welcome you to read our joint proposal and give feedback over the next few days, and then vote on it at Snapshot.

About Avalanche

Avalanche is a proof-of-stake blockchain, whose aim is to be the fastest "L1" smart contract platform, with the ability to process thousands of transactions per second (TPS), at low cost. Avalanche intends to scale horizontally through the creation of independent blockchains running on dedicated subnets. Avalanche's TVL currently stands at around $12B, making it a top-4 DeFi chain.

Staked AVAX (Avalanche's native token) is illiquid until unstaked. Avalanche requires a minimum staking period of two weeks, and a minimum stake of 25 AVAX if delegating, or 2,000 AVAX for a validator (at current prices around $200k USD).

The staking yield for two weeks' tenure is very low. Hence our solution of liquid staking can allow customers to stake for longer tenure with higher yield, and without sacrificing the liquidity (a one year tenure is similar to the status quo of ETH2 with double digit yield).

Avalanche is thus an ideal candidate for liquid staking: users get liquidity while staking to take advantage of DeFi opportunities on the Avalanche chain, and are no longer forced to trade off staking periods with opportunity cost. The high TVL makes the revenue opportunity for Lido extremely high.

High-Level Technical Overview

Avalanche's multi-chain architecture presents interesting challenges to any team wishing to bring Lido to the platform. It is made up of three distinct blockchains: the Exchange Chain (X-Chain), the Platform Chain (P-Chain), and the Contract Chain (C-Chain).

Limitations of Current Avalanche Technology

Smart contracts are executed on the C-Chain, however staking is performed on the P-Chain, which cannot run custom smart contract code.

Because Avalanche does not yet enable smart contracts to transfer AVAX between chains or to perform staking on the P-Chain, it is not currently possible for a smart contract to move tokens between these chains, meaning that some amount of the process must be custodial to begin with.

We propose a two-stage roadmap, combining the best of what is possible today, with a path to improvements in automation and trust minimisation as Avalanche grows. Both stages assume the creation of an Avalanche C-Chain token (stAVAX), representing staked versions of AVAX. At all stages, code will be open sourced and shared with the community.

Interim Solution: Semi-Custodial Liquid Staking

As with Lido stETH, tokens will accrue rewards as a function of time, removing the need for users to sacrifice liquidity or meet minimum staking value requirements to be able to participate in Avalanche's growing DeFi ecosystem. Additionally, governance over selected validators, fees, other parameters, and matters such as upgrades to the protocol will be carried out by LDO holders.

In the initial version, the subset of operations which cannot yet be managed by smart contracts (such as cross-chain transfers and staking) will be carried out via operations requiring multi-party approval. These approaches will then be phased out as the Avalanche blockchain matures.

Long-Term Solution: Trustless Liquid Staking

The next update to Avalanche (Blueberry) intends to improve cross-chain transfer functionality, with work commencing in Q4 2021. We intend to work closely with Ava Labs to build on this and help add functionality to enable automated cross-chain staking with minimized trust.

This will require a number of improvements to Avalanche to better support cross chain messaging and querying, interchain accounts, remote transfers, and ultimately staking from contracts on the C-Chain.

Timeline estimates

Preliminary work:

- Research and development (October-January 2021)
- Initial tech spec (January 2021-February 2022)

Phase 1: semi-custodial liquid staking

- Development: includes custom MPC solution (January-May 2022)
- Fuji testnet deployment and audit (April-May 2022)
- Mainnet deployment (June 2022)

Phase 2: trustless liquid staking

- Avalanche protocol development
- Trustless staking development
- Fuji testnet deployment and audit
- Mainnet deployment

Migration:

- Migration of v1 users / custodied funds to v2; maintenance, upgrades and support for v2 and planning for further iterations

Competitive Landscape

Multiple companies have signaled their intention to build liquid staking for Avalanche. These include:

- BENQI

, a newcomer to the DeFi scene who currently offer borrowing and lending capabilities similar to Compound.

- Ankr

, an established blockchain infrastructure company who aim to offer products, such as staking, on multiple chains.

- Lavax

, which appears to be an effort by independent developers, but with little detail on architecture or timelines.

Of these, only Ankr appears to have already launched their liquid staking solution, albeit with little apparent market liquidity.

Despite not being the first to market with liquid staking on Avalanche, Lido has many advantages over potential competitors, including being a trusted, well-known name in DeFi. If Lido were to bring their liquid staking product to Avalanche, they could potentially capture a share of the market on brand name alone. However, that isn't the endgame.

All companies building liquid staking solutions on Avalanche right now face the same challenges regarding custodianship and trustlessness; none have been open about the architecture of their solutions; and many may feel that their current product is good enough to continue with in the future.

We are certain that Lido entering the market as an established competitor, with its characteristic transparency on current solutions and signaling intention to work towards a better solution with the Avalanche team, will help capture a majority of market share.

Compensation

We believe in the long term success and value proposition of Lido, and are therefore eager to propose a two-part incentive structure that shows our commitment both to this project and to the alignment of our respective interests.

This proposal contains a significant amount of development work, including an interim MPC solution, which contributes to the Lido codebase as a general purpose secure custodial solution, as well as protocol-level development to enhance the cross chain communication on Avalanche.

In this particular implementation for Avalanche, we will tackle the full complexity of the threshold ECDSA, which is more difficult than other setups such as BLS. We foresee a lot of learning and development from this proposal can be applied to other blockchains in the future since these are common challenges for a secure liquid staking solution.

We have modelled our proposal somewhat on Shard Labs' (Polygon) proposal, whose grants were 1M LDO (LDO was trading between $3 and $7 USD during this period).

First, we would propose incentives of LDO tokens with the following terms:

- The initial grant is issued immediately. Subsequent grants are issued when Lido for Avalanche captures % market share, based on the table below.
- A grant given on the basis of delivering Phase 2 of the proposal, which represents a significant amount of potentially uncompensated work on the Avalanche protocol in tandem with the Ava Labs team.

We strongly believe this latter phase will benefit Lido, due to the optics of giving back to the Avalanche developer community and improving the protocol (i.e. supporting trustless inter-chain movements) for all teams working in Avalanche DeFi.

Milestone

LDO

Initial grant, covering delivery of Phase 1

350,000

1% market share

200,000

2%

200,000

3%

200,000

4%

200,000

5%

200,000

10%

500,000

Delivery of Phase 2

150,000

Total

2,000,000 LDO

We define “market share” as the ratio between the amount of staked AVAX tokens via Lido vs. that of all staked AVAX tokens (currently around 60% of supply), based on Avalanche’s Validator Stats page. To qualify, the given market share must be held on average across at least 30 days, to account for variability in the data.

In addition, we propose that audit during the initial grant phase be compensated separately by Lido, and that the Hyperelliptic Labs x RockX team receive 20% of the ongoing Lido treasury fees from this solution, in order to align both parties’ incentives.

An ongoing revenue share plays many roles, including rewarding the team for the success of the project, and in order to cover the costs of ongoing maintenance, improvements, and integrations, both of the solution itself, and of a secure MPC key management system.

Project Team

The project will be jointly carried out by the Hyperelliptic and RockX teams, both of whom will bring their respective strengths to bear on this project.

RockX is an institutional staking service provider, which has been a node operator of stETH and stSOL under Lido. Besides offering institutional staking services and stable access nodes. The team has a research arm X-matrix labs, which specializes in improving defi protocols and developing MPC key management (including DKG, resharing and signing)

The Hyperelliptic Labs team specializes in infrastructure, security and cryptographic key management. The team comes from both crypto and tradfi backgrounds, having built products used by millions of people around the world.

We are in close contact with both core Avalanche and Lido development teams, and look forward to collaborating with them to deliver this solution.