Related to Interchain Liquidity for stTokens.

Summary

Axelar and Hadron Labs are collaboratively bridging wstETH to the Cosmos ecosystem.

The bridge implementation is designed to allow the eventual transfer of ownership of the bridge mechanism to the DAO's Aragon smart-contract, and to prevent the challenges that uncoordinated bridging to the Cosmos ecosystem could result in.

This post summarises the bridge implementation and roadmap. High level implementation strategy for wstETH in Cosmos will be shared subsquently.

Problem statement

Mounting demand for wstETH in Cosmos has been demonstrated by numerous parallel initiatives to bridge the token into the ecosystem. To mention a few:

- Canto bridged wstETH to its ecosystem via custom fork of the Gravity Bridge,
- Injective had plans to bridge wstETH to Cosmos via Wormhole,
- Osmosis and Axelar had plans to bridge wstETH to Cosmos via Axelar.

These demonstrate strong demand for the asset. Nevertheless, left unattended, the resulting uncoordinated bridging outcomes would have present the following long-term issues for wstETH and Lido in Cosmos:

- Vendor lock-in: Migrating to another provider or a different solution a posteriori would generate additional risk and overhead,
- Liquidity fragmentation: denominations being issued by third party bridges would not be fungible with one another, and neither would IBC denominations issued on different chains,
- Technical debt: additional features and upgrades would depend on the goodwill or the various bridge providers and could have led to duplicate work being required to release gas-less bridging or native staking, for example.
- Uneven security: bridges vary wildly in security model and assumptions. Uncoordinated bridging outcomes could have heightened the risk of exploits and loss.

Solution

To alleviate the concerns with uncoordinated bridging outcomes, Lido Protocol Relations contributors and Hadron Labs (a core contributor to Neutron) collaboratively carried out the following steps:

1. Negotiated with Osmosis and Injective to pause uncoordinated bridging attempts
2. Identified bridge providers and solicited proposals
3. Conducted and gathered assessments of the bridge providers
4. Reached out to DeFi projects and put together an integration roadmap
5. Collaborated on defining redlines and a multi-bridge solution spec
6. Gathered supporting economic commitments from bridge providers@

This document outlines the results of this process, which includes the deployment of an initial bridge mechanism to satisfy the urgent demand in the ecosystem and maintain security and optionality for the DAO.

This initial bridge mechanism relies on an established bridging provider, Axelar, and a "wrapper contract" which enshrines a unique denomination for wstETH in Cosmos regardless of what mechanism is used in the backend to enable the bridging of the asset between ecosystems. This contract will initially be owned by a multisig of Cosmos ecosystem contributors, until the contract's ownership can be transferred to the Lido DAO's Aragon smart-contracts on Ethereum, once cross-chain governance has been implemented.

The wrapper contract also enables bridge providers to be added, removed or replaced upon request of the Lido DAO in order to adhere to its security criteria and long-term bridging vision, while avoiding liquidity fragmentation and technical debt.

To ensure this denomination is recognized as the canonical denomination and serves as the shelling point for wstETH

integrations and liquidity in the Cosmos ecosystem, Axelar and Hadron Labs will be collaborating to drive and incentivize the adoption of the token.

Timeline

Hadron Labs believes the following tentative timeline to be realistic:

Sept. 2023:

1. Initial bridge Launch

H1 2024:

1. Cross-chain governance implementation
2. Multi-bridge implementation

Technical Implementation

The initial bridge implementation comprises two components: the Axelar network and a dedicated wrapper contract deployed on Neutron.

Axelar Network

Axelar is a full-stack decentralised transport layer, governed by permissionless PoS consensus. It provides universal composability of programs with any-to-any cross-chain capability. Users access consolidated pools of liquidity. Developers do not need to speak any custom language; they do not need to make any changes to their chains or UIs.

The Axelar Network has three key components across two functional layers.

- The first is the actual network itself, composed of a set of validators that are responsible for maintaining the network and executing transactions. The validators run the cross-chain gateway protocol, which is a multi-party cryptography overlay that sits on top of a Layer 1 blockchain. They are responsible for performing read-and-write operations to gateway accounts deployed on connected external chains, voting, and attesting to events on those chains.
- The second are the gateways, which are effectively smart contracts that provide the connectivity between the Axelar Network and its interconnected external chains. Validators monitor gateways for incoming transactions, which the validators READ. They then come to a consensus on the validity of that transaction and, once agreed, they WRITE to the destination chain's gateway to execute the cross-chain transaction. The funds are sent to a generated address on the source chain and are locked, and a corresponding asset is minted on the destination chain. The validators and gateways compose the core infrastructure layer.
- Sitting on top of the validators and gateways are the APIs that enable developers to access the tools and infrastructure enabled by those validators and gateways. This is the application-development layer that applications will interact with to go cross-chain. It uses the underlying core infrastructure layer to pass customizable, generalised messages across chains. These APIs are how developers can easily lock, unlock and transfer assets between any two addresses on any two blockchain platforms, execute cross-chain application triggers, and more generally handle any cross-chain requests.

Useful links

- Code
- Docs
- Audits

Security Considerations

- Axelar Admin multisig: The former admin multisig is being deprecated, and replaced with validator voting for all upgrades. The new implementation has been audited, and is planned to go live by the end of August. The code for the governance implementation slated to replace the former admin multisig can be found here.
- AXL token

External Diligence reports

- Uniswap Diligence Report

- LiFi Report

Wrapper Contract

The purpose of the wrapper contract is to serve as a bridge agnostic anchor for the wstETH denomination in Cosmos. It allows bridge providers to be swapped in and out without needing to deploy swap contracts or rebuild liquidity.

Initially, the contract will be owned on behalf of the Lido DAO by a multisig of Cosmos contributors. The multisig is expected to be deprecated in favour of the Aragon smart-contracts of the Lido DAO once cross-chain governance is implemented, tested and audited.

Individual

Project

Address

Kai Tyurin

Hadron Labs

neutron1tkavhfqt8358vl74z7r5kdkdy05s98yka0gl0t

Avril Dutheil

Neutron Foundation

neutron1yycmdn4t5gmzfddtsle2xurd3x30h4crz02j9x

Georgios

Axelar

neutron1pymharqxfutl5ncpxe8hghpsz4y39jxl8wlfd0

Robinson Burkey

Wormhole

neutron17venextdsudmg96v8kp70c83zlk25y9cwqlwv2

Mirza Uddin

Injective

neutron1gdzdhhndw5jsdvt8cdzk2xuy0w4nprrp5lwppp

In the future, once available, the contract may be upgraded intoa multi-bridge solution without changing the denomination. This would provide better security guarantees than any single bridge provider and would make the setup resistant to the failure of a portion of the bridges.

Useful links

- Code
- Audit
- Bridge agnostic spec