Introduction

In response to the Lido community's call for a secure and transparent expansion of wstETH to the BNB chain, Axelar Inc. and Wormhole present a unified proposal that leverages the expertise and technology of Wormhole, Axelar network, and the Lido DAO. This proposal aims to establish a multi-bridge deployment that adheres to Lido's governance processes, ensures the DAO's ownership and control, provides vendor flexibility, and addresses network-specific considerations. This proposal is based on a collaborative effort that aligns with the Lido community's values of decentralization, transparency, and openness.

We'd like to express our thanks to the Lido Network Expansion Workgroup (NEW) for their feedback as we've put together this design. Should it receive positive community feedback and DAO approval, Axelar Inc. and the Wormhole Network will jointly deploy the Lido wstETH bridge to BNB Chain.

Problem Background

To bridge wstETH to a new ecosystem, the solution should encompass:

- Robust Security

: Similar to blockchain consensus protocols, cross-chain systems need to prioritize safety and operational continuity.

- Liveness

: It must support transaction completion within a reasonable timeframe.

- Decentralization

: Decentralization is critical for ensuring both safety and liveness.

- Unified wstETH Representation

: A single, Lido DAO-authorized representation of wstETH should exist across the BNB chain and be recognized by all dApps in that ecosystem.

- Governance by Lido DAO

: The governance of new wstETH contracts should be fully controlled by Lido DAO's Aragon governance contracts on the Ethereum mainnet. This includes the ability to modify messaging network providers to maintain top-tier security standards.

Technical Overview

We propose a multi-bridge approach that combines Wormhole and Axelar network messaging in a standardized way, and provides the Lido DAO flexibility to add more messaging providers in the future.

Below is a high-level diagram of the entire flow:

[

Wormhole-Axelar

617×525 11 KB

](https://europe1.discourse-cdn.com/business20/uploads/lido/original/2X/e/e39eb8c4a5f0820cad2fd662d730e24f9d895d34.png)

The main components are:

- BridgeManager
- responsible for locking and minting wstETH, governance, and sending/receiving multi-bridge messages via the Endpoint

components

- Endpoint
- responsible for sending and receiving cross-chain messages from a single provider
- wstETH

on BNB - newly deployed ERC20Burnable

(or similar) representing wstETH on BNB

When a user transfers wstETH from Ethereum to BNB, the following steps occur:

1. The user interacts with the BridgeManager

contract. This contract locks the user's wstETH and sends messages to mint wstETH on BNB via each Endpoint

contract. In this design, Axelar and Wormhole each implement an Endpoint

contract and the Lido DAO can choose to modify or add additional messaging providers.

1. Each messaging provider will perform its own verification of the message from Ethereum and relay attestations to the corresponding Endpoint

contract on BNB. At a high level: * Wormhole's validators (Guardians) identify messages emitted from Ethereum, wait for finality, and produce a signed attestation once a super-majority come to consensus. A Wormhole relayer then delivers this message to the Wormhole Endpoint

on BNB.

- Axelar network is a decentralized Proof-of-Stake based network that leverages a distributed consensus to verify and route messages across chains. Once the message is posted on the source chain, the validators verify it, route it, and a relayer transmits a transaction to the destination chain approving the cross-chain message.
- Wormhole's validators (Guardians) identify messages emitted from Ethereum, wait for finality, and produce a signed attestation once a super-majority come to consensus. A Wormhole relayer then delivers this message to the Wormhole Endpoint

on BNB.

1. Axelar network is a decentralized Proof-of-Stake based network that leverages a distributed consensus to verify and route messages across chains. Once the message is posted on the source chain, the validators verify it, route it, and a relayer transmits a transaction to the destination chain approving the cross-chain message.
2. Endpoint

contracts on BNB Chain receive and verify their respective messages and then the BridgeManager

aggregates these messages and verifies that the appropriate 2-of-2 threshold is met. If all checks pass, the BridgeManager

mints wstETH and delivers it to the intended recipient.

When a user transfers wstETH from BNB to Ethereum, similar steps occur with the following exceptions:

- The BridgeManager

on BNB will burn the user's wstETH, instead of locking. This is because BNB wstETH will be a newly deployed ERC20Burnable

(or similar) that can be burned.

- The BridgeManager

on Ethereum will unlock and send wstETH to the recipient, instead of minting. This is because wstETH on Ethereum cannot be minted outside of Lido's wrapping flow.

This design is flexible and the Lido DAO can choose to add more Endpoint

providers or update the multi-bridge threshold, e.g. from 2-of-2 to 2-of-3 or 3-of-3.

Cross-Chain Governance

The Lido DAO can perform cross-chain governance via this multi-bridge design. Other BridgeManagerMessage.type

values can be used to communicate governance messages. Lido contributors have full flexibility in determining what kind of governance messages to support and how the payloads for those messages should be defined.

Initial Contract Ownership

Wormhole will deploy the BridgeManager

, Endpoint

, and wstETH contracts on the BNB network. Following the deployment, ownership of these contracts will be transferred to a multi-sig composed of contributors from the Axelar network decentralized governance module secured by the entire Axelar network, the Wormhole Foundation, and a represented elected by BNB chain officials. This multi-sig arrangement is intended as a temporary measure. Once cross-chain governance has been implemented, thoroughly tested, and audited, the multi-sig will be phased out in favor of the Aragon-based smart contracts controlled by the Lido DAO.

Governance and Ownership:

Lido DAO's Aragon governance contracts will maintain full control over the wstETH contracts, with the ability to add or remove messaging providers as the technology advances.

Security and Operational Considerations:

Security is paramount, and this proposal joins the security measures of Wormhole and Axelar network together to protect Lido users. Axelar network implements multi-layered security starting with the decentralized protocol, followed by robust engineering, and application-level addons and the Wormhole network incorporates defense-in-depth measures like the Global Accountant and Governor. Both protocols have undergone extensive audits and maintain large public bug bounties to maintain high security and operational standards.

While a multi-bridge approach is subject to the combined uptime of all providers, Wormhole and the Axelar network are both designed with resilience in mind and have encountered no significant downtime in the past year.

Wormhole:

- Audits: wormhole/SECURITY.md at main · wormhole-foundation/wormhole · GitHub
- Bug bounty: Wormhole Bug Bounties | Immunefi
- Security overview: Cross-chain security | Wormhole

The Axelar network:

- Audits: GitHub - axelarnetwork/audits: Axelar network audits
- Bug bounty: Axelar Network Bug Bounties | Immunefi
- Security overview: https://axelar.network/blog/security-at-axelar-core

Funding and Support:

Axelar, inc. and Wormhole do not seek funding from Lido DAO for engineering expenses related to the multi-bridge implementation. Both bridge providers will independently bear the engineering and auditing costs for this public good.

Timeline and Next Steps:

Wormhole and Axelar Inc. have started implementing the multi-bridge messaging framework and estimate the following timelines:

- 2023-12-08: Initial implementation code complete and ready for audits
- 2023-12-22: Audits by internal security researchers complete and feedback addressed
- 2024-01-12: Audits by external auditing firms complete and feedback addressed
- 2024-01-15: Testing period starts with Wormhole deploying bridge to BNB
- 2024-01-29: Axelar network is added to multi-bridge and threshold is updated to 2-of-2

The timeline includes a two-week test period on the BNB chain with Wormhole's deployment, followed by Axelar network integration.

Call to Action:

In response to the Lido DAO's RFP, we'd like to invite the community to examine this proposal, offer feedback, and engage in the upcoming governance vote. With your support, we can ensure that wstETH's expansion to BNB is executed with the highest standards and community governance

About Axelar

Axelar network is the leading interoperability layer for Web3. The network enables blockchain as a new kind of development platform, integrating diverse networks into a seamless "Internet of blockchains." Axelar is programmable and decentralized, secured by a proof-of-stake token, AXL. Application users access any digital asset or application, with one click. Developers work with a simple API and access an ecosystem of tools and service providers.

Axelar is funded by top-tier investors, including Binance, Coinbase, Dragonfly Capital, Galaxy and Polychain Capital. Major partnerships and integrations include Microsoft, Mastercard, JPM, dYdX and Uniswap. Axelar's team includes experts in distributed systems/cryptography and MIT/Google/Consensys alumni; the co-founders, Sergey Gorbunov and Georgios Vlachos, were founding team members at Algorand.

About Wormhole

Wormhole is the longest-running generic cross-chain messaging protocol, with the first production message sent in August 2021. Hundreds of projects have leveraged Wormhole to transfer over 35 billion USD of value and over 750 million messages across more than 30 chains. These messages enable sending price oracle data, transferring tokens between chains, building cross-chain DeFi protocols, cross-chain governance, and many other use cases.

Additionally, Wormhole was named the only unconditionally approved protocol by the Uniswap Foundation's Bridge Assessment Committee — Bridge Assessment Report.