Deploy wstETH to BNB Chain Using Chainlink CCIP

Abstract

This proposal aims to make Lido's Wrapped Staked Ether (wstETH) token available on BNB Chain by using the Chainlink Cross-Chain Interoperability Protocol (CCIP). CCIP offers the highest level of cross-chain security for Lido by utilizing multiple Decentralized Oracle Networks (DONs), an independent Risk Management Network, high-quality node operators, and additional security features such as rate limiting.

This proposal presents a balanced approach that combines the strong security guarantees of Chainlink CCIP's lock-and-mint token transfer mechanism as the default configuration with the flexibility of a configurable token pool contract owned by the Lido DAO.

Rationale

The DeFi ecosystem now exists within a multi-chain world, composed of a growing collection of different and disconnected blockchain environments. Making Lido Staked Ether (stETH) more widely available to users and dApps across non-Ethereum blockchains will directly expand the utility of both Lido and the DeFi ecosystem at large.

However, given the historical amount of value exploited by insecure cross-chain bridge protocols ($2.7B+), and the significant and growing amount of value secured by stETH ($20B+), Lido requires the most secure cross-chain interoperability protocol. We believe that Chainlink CCIP serves as the optimal solution to support Lido's cross-chain expansion.

This proposal is focused on making wstETH available on BNB Chain, resolving liquidity fragmentation issues through a canonical deployment. However, in future proposals to the Lido DAO, the use of CCIP could potentially be expanded to support additional chains for cross-chain wstETH, enable users to stake ETH directly from other networks, support automated cross-chain governance processes, provide access to institutions' and capital markets' tokenization initiatives, or even power other forms of cross-chain coordination for the Lido ecosystem.

Chainlink Background

Chainlink is a blockchain-agnostic, decentralized computing platform that provides secure access to external data, offchain computation, and cross-chain interoperability. Historically, Chainlink has supported the growth and adoption of Lido through the deployment of 11 Price Feed oracle networks across five blockchains that provide market-wide exchange rates around stETH, which have collectively enabled over $193B in transaction value since the beginning of 2022. These Price Feeds are used by widely-adopted protocols within the multi-chain DeFi ecosystem, including Aave with $3B+ of wstETH deposited as collateral which combines wstETH/stETH Exchange Rate feeds or onchain exchange rate value with stETH/USD Price Feeds.

Chainlink CCIP serves as an interoperability standard for transferring both tokens and/or data between any public or private blockchain network. CCIP supports Ethereum, Polygon, Avalanche, Arbitrum, Optimism, BNB Chain, and Base, with support for more chains planned to be added over time. Over 80 DeFi protocols have integrated or are integrating CCIP for cross-chain token transfers and/or cross-chain messaging. This includes Synthetix's use of CCIP for cross-chain transfer of sUSD via the Synthetix Teleporter (Burn and Mint), as well as Aave's use of CCIP for cross-chain governance.

Beyond DeFi, Chainlink Labs has collaborated with some of the world's largest financial institutions, market infrastructure providers, and enterprises on how CCIP can securely facilitate the cross-chain settlement of tokenized assets across public/private chains. This includes work with Swift (interbank messaging standard for 11,000+ global banks), DTCC (settles $2+ quadrillion in securities volume annually), ANZ ($1T+ assets under management), and Vodafone DAB (IoT-enabled global trade platform).

Developed with security and reliability as the primary focus by some of the industry's leading academic researchers, CCIP operates at the highest level of cross-chain security. CCIP's defense-in-depth security and suitability for the Lido ecosystem can be broken down across four categories:

Multiple Layers of Decentralization

CCIP is underpinned by Chainlink's proven decentralized oracle infrastructure, which has enabled over $9.2T in transaction value within DeFi since the beginning of 2022. Rather than operating as a single monolithic network, CCIP is composed of multiple decentralized oracle networks (DONs) per chain lane, each consisting of a unique source chain and destination chain. This approach allows CCIP to be horizontally scalable, as additional DONs are added to CCIP for each additional blockchain network supported, versus funneling all cross-chain traffic through a single network.

The committing DON is a decentralized network of oracle nodes that monitor events on a given source chain, wait for source chain finality, bundle transactions to create a Merkle root, come to consensus on that Merkle root and finally commit that Merkle root to the destination chain. The executing DON is a decentralized network of oracle nodes that submit Merkle

proofs on a destination chain, which is then verified onchain by ensuring the transactions were included in a previously committed Merkle root that has been validated by the Risk Management Network.

[

CCIP_Architecture

1600×900 157 KB

](https://europe1.discourse-cdn.com/business20/uploads/lido/original/2X/4/423025e61d6712a62948f1111f4c831907b89010.png)

Risk Management Network

The Risk Management Network is a separate, independent network that continuously monitors and validates the behavior of CCIP, providing an additional layer of security by independently verifying cross-chain operations for anomalous activity. The Risk Management Network utilizes a separate, minimal implementation of the Chainlink node software, creating a form of client diversity for increased robustness while also minimizing external dependencies to prevent supply chain attacks.

More specifically, the Risk Management Network was written in a different programming language (Rust) than the primary CCIP system (Golang), developed by a different internal team, and uses a distinct non-overlapping set of node operators compared to the CCIP DONs. The Risk Management Network is a wholly unique concept in cross-chain interoperability that builds upon established engineering principles (N-version programming) seen in mission-critical systems in industries such as aviation, nuclear, and machine automation.

To increase the security and robustness of CCIP, the Risk Management Network engages in two types of activities:

- Secondary Approval:

The Risk Management Network independently recreates Merkle roots based on transactions from the source chain, which are then published on the destination chain and compared against the Merkle roots published by the Committing DON. Cross-chain transactions can only be executed if the Merkle roots from the two networks match.

- Anomaly Detection:

The Risk Management Network monitors for abnormal behavior from the CCIP network (e.g., committed transactions with no source chain equivalent) as well as the behavior of chains (e.g., deep block reorgs). If suspicious activity is detected, the Risk Management Network can trigger an emergency halt to pause all CCIP lanes and limit any losses.

High-Quality Node Operators

Chainlink DONs are operated by a geographically distributed collection of Sybil-resistant, security-reviewed node operators with significant experience running mission-critical infrastructure across Web2 and Web3. Node operators in the Chainlink ecosystem include global enterprises (e.g., Deutsche Telekom MMS, Swisscom, Vodafone), leading Web3 DevOps teams (e.g. Infura, Coinbase Cloud), and experienced Chainlink ecosystem projects.

Many of the node operators that actively secure Chainlink Data Feeds also already run Lido validators including Blockdaemon, Chainlayer, Chorus One, Cryptomanufaktur, Everstake, Figment, Infinity Stones, P2P, Stakefish, Stakin, and Staking Facilities. A number of node operators securing CCIP similarly also operate Lido validators, minimizing trust assumptions for the Lido ecosystem.

The Committing DONs and Executing DONs in CCIP are composed of 16 high-quality independent node operators, while the Risk Management Network is composed of 7 distinct node operators (resulting in a total of 23 node operators). Importantly, the Risk Management Network consists of a wholly separate and non-overlapping set of nodes compared to the primary CCIP networks, helping ensure independent secondary validation. As the value secured by CCIP expands over time, the number of node operators within each network can scale to meet the need for greater security.

Configurable Rate Limits

As an additional layer of security for cross-chain token transfers, CCIP implements configurable rate limits, established on a per-token and per-lane basis, which are set up in alignment with the token contract owners like Lido. Furthermore, CCIP token transfers also benefit from the increased security provided by an aggregate rate limit (across token pools) on each lane, so even in a worst-case scenario, it would be impossible for every token's limit to be maxed out before the aggregate rate limit on a lane is hit.

Implementation

1. On behalf of Lido DAO, Chainlink Labs deploys the wstETH token contracts on the relevant chains (i.e., BNB Chain), which Lido DAO will own and control

2. On Ethereum:
3. wstETH Token Contract:
4. No modification or wrapping is required for the existing wstETH token contract
5. No modification or wrapping is required for the existing wstETH token contract
6. Token Pool Contract:
7. On behalf of Lido DAO, Chainlink Labs will deploy a lock/release token pool contract. Ownership of the token pool is transferred to Lido DAO.
8. Lido DAO will own and control this token pool contract
9. Lido DAO sets per-lane rate limits on the token pool contract, i.e.
10. Individual rate limits to lock tokens per destination.
11. Individual rate limits to release tokens per source.
12. Individual rate limits to lock tokens per destination.
13. Individual rate limits to release tokens per source.
14. Lido DAO grants CCIP the bridge role on the token pool contract
15. With the bridge role, CCIP sets permissioned addresses that can call lock()

or release()

- There are no liquidity providers, all liquidity in the pool comes from tokens being locked for bridging.
- On behalf of Lido DAO, Chainlink Labs will deploy a lock/release token pool contract. Ownership of the token pool is transferred to Lido DAO.
- Lido DAO will own and control this token pool contract
- Lido DAO sets per-lane rate limits on the token pool contract, i.e.
- Individual rate limits to lock tokens per destination.
- Individual rate limits to release tokens per source.
- Individual rate limits to lock tokens per destination.
- Individual rate limits to release tokens per source.
- Lido DAO grants CCIP the bridge role on the token pool contract
- With the bridge role, CCIP sets permissioned addresses that can call lock()

or release()

- There are no liquidity providers, all liquidity in the pool comes from tokens being locked for bridging.
- In order to migrate, the owner of the pool can call migrateLiquidity()

to transfer all locked tokens to a new pool.

1. On BNB Chain:
2. wstETH Token Contract:
3. On behalf of Lido DAO, Chainlink Labs deploys a new canonical wstETH token contract. Ownership of the token contract is transferred to Lido DAO.
4. Lido DAO will own and control the wstETH token contract on BNB Chain.
5. On behalf of Lido DAO, Chainlink Labs deploys a new canonical wstETH token contract. Ownership of the token contract is transferred to Lido DAO.
6. Lido DAO will own and control the wstETH token contract on BNB Chain.

7. Token Pool Contract:
8. On behalf of Lido DAO, Chainlink Labs will deploy a burn/mint token pool contract, which Lido DAO will own and control.
9. The pool will burn tokens on BNB Chain to be released on Ethereum.
10. The pool is whitelisted to burn and mint wstETH
11. Lido DAO sets per-lane rate limits, i.e.
12. Individual rate limits to burn tokens per destination.
13. Individual rate limits to mint tokens per source
14. Individual rate limits to burn tokens per destination.
15. Individual rate limits to mint tokens per source
16. Lido DAO grants CCIP the bridge role on the token pool contract
17. With the bridge role, CCIP sets the permissioned addresses that can call burn()

or mint()

.

- On behalf of Lido DAO, Chainlink Labs will deploy a burn/mint token pool contract, which Lido DAO will own and control.
- The pool will burn tokens on BNB Chain to be released on Ethereum.
- The pool is whitelisted to burn and mint wstETH
- Lido DAO sets per-lane rate limits, i.e.
- Individual rate limits to burn tokens per destination.
- Individual rate limits to mint tokens per source
- Individual rate limits to burn tokens per destination.
- Individual rate limits to mint tokens per source
- Lido DAO grants CCIP the bridge role on the token pool contract
- With the bridge role, CCIP sets the permissioned addresses that can call burn()

or mint()

.

1. Advantages of this approach:
2. wstETH Token Flexibility:

CCIP only needs the token to have permissioned burn/mint functions on BNB Chain. The token does not contain any bridging logic, or any bridge trust assumptions.

- Per-lane Rate Limit:

Lido DAO can adjust rate limits for each chain based on its level of security.

1. Note:
2. CCIP implements an aggregate rate limit at the lane level (global for all tokens transferable on that lane). This is separate from the wstETH-specific rate limit that the Lido DAO would configure on the wstETH token pools for each lane.

[

CCIP Lido Proposal Diagrams_ETH-BNB_1

4001×2250 170 KB

](https://europe1.discourse-cdn.com/business20/uploads/lido/original/2X/3/3f6c4c47cd10294a30f36fe6db0585e827041c39.png)

[

CCIP Lido Proposal Diagrams_ETH-BNB_2

4001×2251 170 KB

](https://europe1.discourse-cdn.com/business20/uploads/lido/original/2X/2/2acd601ba92c8da0ce9ba90c999360e697edf5dc.png)

Audits and Source Code

Security is the number one priority for the Chainlink ecosystem, a value we do not and will not compromise upon. Chainlink Labs has put an immense amount of resources into developing the security model of CCIP, and as such, is the most audited Chainlink solution to date.

Both the onchain and offchain code for CCIP and the Risk Management Network was subjected to 14 independent audits by five leading security firms (Cure53, Dedaub, NCC Cryptography Services, Sigma Prime, and Trail of Bits) in preparation for the initial mainnet launch.

Additionally, two crowdsourced audits of CCIP and the Risk Management Network were conducted on theCode4rena (C4) platform:

- CCIP and Risk Management Network
- CCIP Administration Contracts

All valid findings were remediated and fixes confirmed with the respective auditors. In some cases, findings represented expected behaviors and were reviewed with auditors upon receipt of audit reports.

The source code for CCIP is publicly viewable on GitHub:

- Cross-Chain Interoperability Protocol
- Risk Management Network
- CCIP Owner Contracts

Information on the software license of CCIP can be found on the CCIP GitHubhere and here.

Upgradability

All on-chain security-critical configuration changes and upgrades to CCIP must pass through a Role-Based Access Control Timelock (RBACTimelock) smart contract.

Any proposal must either (1) be proposed by a dedicated ManyChainMultiSig contract and then be subjected to a review period, during which the node operators securing CCIP are able to veto the proposal; or (2) be proposed by a dedicated ManyChainMultiSig contract and be explicitly approved by a quorum of the node operators securing CCIP, providing an alternative path during time-sensitive circumstances.

Any onchain update that passes the timelock without a veto becomes executable by anyone, which can be done by running a timelock-worker to process executable upgrades.

Documentation and source code relating to the CCIP owner contracts can be read on GitHub. The proposer multisig on Ethereum can be found on Etherscan, where configuration details can be read.

Economics

CCIP uses a gas-locked fee payment mechanism, called Smart Execution, to help ensure the reliable execution of cross-chain transactions regardless of destination chain fee spikes. Users only need to pay a single one-time fee on the source chain, while CCIP handles end-to-end execution and gas management.

The payment/billing model of CCIP was designed to reduce friction for users and allow the protocol to quickly scale to additional blockchain networks. As such, CCIP supports fee payments in LINK and in alternative assets, which currently take the form of blockchain-native gas tokens and their ERC20 wrapped versions (e.g., LINK, WBNB, and BNB for BNB Chain). Users do not need to call any functions on the destination chain, as the DONs call the mint/release functions (as applicable) on the destination chains. For cross-chain token transfers, CCIP fees encapsulate both the gas cost overhead incurred on the destination chain, as well as a percentage-based fee premium based on the amount of value transferred. A

percentage-based fee premium helps ensure an equitable distribution of security cost across the users, where higher value transactions contribute a higher percentage of fees that support the security of CCIP.

As transaction volumes scale for the given chain-lane (e.g. Ethereum <> BNB Chain), a positive flywheel effect is created where an increase in aggregate fees can then be used to increase the security guarantees of CCIP, such as adding more node operators, enabling the protocol to secure a greater amount of transaction volume. This scalable approach to security can be seen across Chainlink Price Feeds, which have enabled over $9.2T in transaction value enabled within DeFi.

Current CCIP premium fees are in line with industry standards within the cross-chain ecosystem, but these values are subject to change. The premium portion of fees paid in alternative assets have a surcharge of 10% when compared to LINK payments. Work is underway on a Payment Abstraction solution where fee payments made in alternative assets are turned into LINK to reward network service providers.

Chainlink Labs is not requesting any funding to implement wstETH token transfers to BNB Chain using CCIP.

Next Steps

We are thrilled about the opportunity to help Lido securely achieve its cross-chain vision. We want to give our appreciation to the Network Expansion Workgroup (NEW) for providing meaningful feedback to help improve the proposal.

Integrating Chainlink CCIP for cross-chain token transfers of wstETH on BNB Chain presents a unique opportunity to expand both the utility and accessibility of Lido Staked Ether across the multi-chain DeFi ecosystem using highly secure and robust cross-chain infrastructure. After a community discussion period, a temperature check will take place on Snapshot before an on-chain vote.

Disclaimer

Chainlink Labs' work is offered "as is" without representations, guarantees, or warranties of any kind, on a commercially feasible basis and subject to Lido DAO's acceptance of the Chainlink Labs terms of service (available at Terms of Service – Chainlink Labs). The benefits are solely being made available to the Lido Protocol and not to any other party, including Lido DAO.