Summary

This proposal seeks DAO consideration for xERC20, the open crosschain token standard, and its adoption for wstETH.

The objective is to solve many of the core frictions of bridging wstETH across networks in a permanent way.

This approach tackles the following challenges:

- Ensure the Lido DAO retains ownership and control over their token contracts across different chains and bridges.
- Provide the Lido DAO the flexibility to add and remove bridges at will over time, with desired minting rate limits
- Bring wstETH to 1000 rollups in the most capital efficient way

xERC20 is an open crosschain standard (EIP 7281) that allows any bridge to work with Lido.

We believe it is a massive improvement in security, sovereignty, and UX over proprietary approaches or self-made architectures. LidoDAO has previously used a similar strategy to deploy wstETH on Optimism and Arbitrum.The xERC20 represents a broader version of this approach.

Overview

To bridge wstETH, there must be at least one representation of wstETH on the target chain.

The LidoDAO has chosen to deploy a custom wstETH token contract on each chain and build a communication channel on top of the L2 native bridges.

This is highly secure as it is using L2 native bridges, but it has the below tradeoffs

- Bridging is typically slow/expensive
- Only connected to Ethereum.
- Does not allow for crosschain actions (ex: crosschain staking)
- Requires custom work on every chain.

The last point is critical: using this architecture is quite effective for a limited number of L2s.

But how can the Lido DAO scale its products to 100, 10000 or more rollups?

As the Lido DAO has already recognized the need for fast L2<>L2 bridging, a current system of AMM pools on each chain enables the movement of wstETH by using a 3rd party bridge. This architecture, while being the only possible way for the current construction, is not the most capital efficient, and implies that user transfers always incur into slippage.

When looking at crosschain token transactions, there are 3 options that Lido can adopt:

Crosschain Approach

Pros

Cons

1

Lock in with a single provider

wstETH can be transferred with no slippage on all chains, for any number of chains

wsETH (and by extension, Ethereum) now faces a systemic risk through the bridge provider.

2a

Lido DAO does not endorse any option - on an L2

Canonical bridged asset becomes canonical

Every bridge must build liquidity (or Lido must pay for this). wstETH transfers incur slippage, breaking composability. Does not scale to many chains

2b

Lido DAO does not endorse any option - on new L1

Free market: every bridge can move their version of wstETH

Fragmented, awful UX

3

xERC20

All of the above; Any bridge can work with the LidoDAO if whitelisted. Granular risk control. Enables crosschain operations

Requires active governance.

What is xERC20?

xERC20 (ERC-7281) tokens are ERC-20 tokens which can be transferred with no slippage across chains without compromising on security.

Contrary to other proprietary crosschain standards, token issuers always retain control and sovereignty over their tokens. This ability would allow the Lido DAO to whitelist specific bridges, giving them the rights to mint the same representation of the crosschain token. The xERC20 standard allows token issuers to exert fine-grained control over security preferences, as the LidoDAO can set rate limits on minting/burning operations for each bridge, enhancing security measures and limiting potential damage in the event of security breaches.

The Lido DAO can tailor these controls to align with its risk tolerance and operational requirements.

xERC20s are neutral, native crosschain tokens to satisfy the business needs of projects today while being future proof for the technology of tomorrow.

An extensive number of bridges including Li. Fi, Chainsafe, Hashi, Across, Socket and Connext has already committed to supporting open standards and an open approach.

Importantly, the xERC20 standard is fully functional even with bridges that haven't explicitly signaled support:

for example, BEEFY has upgraded its token to xERC20 and whitelisted Axelar, CCIP, and LayerZero.

What are the advantages?

While we recognize the value that a security-first approach using only native bridges provides, we believe there is an opportunity for a flexible approach that combines rollups bridges with 3rd party bridges with conservative minting rights.

- Capital efficiency

: enables 0 slippage crosschain movements without any requirement to bootstrap liquidity in advance. No AMMs are required at all.

- Independence and Flexibility

:

xERC20 is a bridge-agnostic open standard, providing token issuers the ability to retain control and sovereignty over their tokens, and the flexibility to change the messaging bridges used over time.

- Consistent User Experience

:

Any proprietary system can lead to inconsistent user experiences when transferring tokens over canonical bridges. Users may receive different versions of the token than intended, causing confusion and disrupting user trust.

The xERC20 standard ensures a seamless and consistent user experience, guaranteeing that users receive the official asset regardless of the bridge used. This includes the native bridges of the chains.

- Granular security control

Security can be isolated per chain, per bridge and minting limits. Since the limits are enforced in the token contracts, you can effectively set per-chain limits as well, simply by having different limits for each bridge on each chain.

The ability to add 3rd party bridges in the whitelist allows users to move tokens out of L2s without using the native bridges, providing a fast experience.

- Faster deployment, enhanced functionalities

Using the xERC20 would allow the LidoDAO to easily and more cost-effectively deploy and launch to 1000 rollups with a simplified process compared to the current one.

Enabling 3party bridges (even with very extremely conservative minting limits) enables fast and cheap transfers of wstETH between L2s (without having to go through Ethereum mainnet), and the opportunities in the future to create crosschain applications on top of the Lido protocol, like, for example, crosschain staking

.

Trade-offs

xERC20 is not a magical silver bullet. In particular, it requires active decision-making, as the DAO (or a delegation) is in charge of assessing the risks of the various bridges and deploying token contracts on each chain.

This is necessary to ensure the LidoDAO is always in control of the token contracts, and a similar architecture isalready in place for current versions of wstETH bridged to Optimism and Arbitrum, where a mono-bridge locked in approach was used.

Risks

xERC-20 smart contracts have been tested and audited; as every smart contract they might be subject to vulnerabilities. However, we believe the risk is low as the standard is a light extension to the ERC-20 interface, and is already used in production by several projects.

What impacts the risk curve are the bridges that get whitelisted.

- If the Lido DAO decides to only whitelist native bridges, this would effectively have the same risk as the current implementation on the L2s.
- If the Lido DAO decides to whitelist other 3rd party bridges, this increases the risk for wstETH. The xERC20 doesn't enhance the security of the single bridge, but it allows to clearly confine the risk exposure for each bridging provider.

We would recommend a cautious approach of gradual whitelisting only the most trust-minimized solutions, with initial small limits that can be gradually increased once the technologies are more ossified and become battle tested.

How it works

xERC20 is a simple extension to the ERC20 interface to add:

- Mint and burn.
- Owner-controlled allowlist to call the above.
- Owner-controlled rate limits and caps on minters and burners.

Why now

The upcoming proliferation of L2s and L3s requires the Lido DAO to be able to expand to multiple ecosystems without having to spend capital for liquidity mining programs while maintaining control over sovereignty and security.

The xERC20 standard becomes the only viable way to foster fast adoption of wstETH across any ecosystem.

How does whitelisting work?

The token issuer of an xERC20 configures rate limits on a per-bridge basis. This gives issuers granular control over their risk appetite and encourages more open competition around security.

In order to whitelist a bridge, the owner of the token contract on each chain needs to call the following function on the xERC20:

- @ notice Updates the limits of any bridge
- @ dev Can only be called by the owner
- @ param _mintingLimit The updated minting limit we are setting to the bridge
- @ param _burningLimit The updated burning limit we are setting to the bridge

- @ param _bridge The address of the bridge we are setting the limits too
- function setLimits(address _bridge, uint256 _mintingLimit, uint256 _burningLimit) external;

The Lido DAO could decide to hold a vote for every chain to whitelist specific bridges, or spin up a specialized whitelisting committee.

An option could be the election of a committee that includes members of the Network Expansion Group, and external 3rd parties with proven ability to research and objectively assess which bridges are best positioned to be whitelisted and with what minting/burning limits.

Implementation Plan

Below are the recommended steps for Lido DAO to adopt the xERC20 standard on a new chain and/or to migrate existing wstETH on existing L2.

We recommend migrating existing assets with native bridges as well in order to maintain implementation consistency, and to best ensure wstETH can be bridged seamlessly across all chains into the future.

Introducing xERC20 support for wstETH on a new chain

This must follow a DAO/committee decision on which bridges should be allowed to mint tokens on the given chain, and with what rate limits, as described above. Limits can be updated by the controlling party at any time.

1. On Ethereum: Deploy xERC20 version of wstETH and deploy the Lockbox
2. On the new chain: Deploy xERC20 version of wstETH
3. Set rate limits for bridge(s) accepted by LidoDAO by callingsetLimits
4. Work with bridge(s) to ensure they mint/burn the new xERC20 token.

Audited contracts can be deployed using the scripts inthis repo. Based on wstETH deployments on other chains, upgradeability may be desired and can be added.

[

1600×541 59.7 KB

](https://europe1.discourse-cdn.com/business20/uploads/lido/original/2X/4/48a82d1de66797a72684da90b410e3fb99a1123e.png)

Migrating existing wstETH on L2 chains to xERC20

1. On Ethereum: Deploy xERC20 version of wstETH and deploy the Lockbox (If these already exist per step 1 of the previous section, then skip this step)
2. On L2(s): Upgrade wstETH to comply with thexERC20 specification
3. Per chain: Set rate limits for bridge(s) accepted by LidoDAO. At current state, this would only involve existing native bridges.
4. Create an adapter for Lido's custom native bridge implementations to deposit/withdraw to and from the Lockbox
5. Migrate liquidity locked in the native bridges to the Lockbox, following LidoDAO approval
6. As LidoDAO controls the native bridge implementations, we suggest to:

A) Send the locked wstETH on each custom token gateway to the Lockbox contract. This consolidates all wstETH liquidity into the Lockbox and removes custody over wstETH from existing bridges (canonical or otherwise).

B) For each chain migrated, it's extremely important to consolidate all locked wstETH into the Lockbox. This ensures liquidity can be accessed from a single shared source and avoids any potential fragmentation for end users.

Once steps to migrate are completed, a typical bridge flow will look as follows:

[

1600×595 81.8 KB

](https://europe1.discourse-

cdn.com/business20/uploads/lido/original/2X/5/5d5eb6387d0111138e59323aef5d5bba79cc4ad5.png)

Next Recommended Steps

- Hold discussion within the Lido community to clarify the benefits of the standard and the best processes to implement it (including the whitelisting process)
- If the community shows early support for this proposal, a first temperature check will be proposed in January
- A detailed implementation plan can be coordinated to migrate tokens on all L2s in the most secure and seamless way possible.