Introduction

Matter Labs proposes the deployment of wstETH (Wrapped staked ETH) to zkSync, with the ultimate goal of acceptance of ownership of the wstETH bridging components by the Lido DAO.

1. zkSync's Rapid Growth and Ecosystem:

This proposal is for wstETH deployment on zkSync Era Mainnet. Our conviction is rooted in the potential which wstETH on zkSync holds to usher in novel use cases within the DeFi ecosystem and stimulate increased demand for wstETH across all channels.

zkSync Era Mainnet is a significant leap forward in Layer 2 technologies with long awaited improvements and benefits for Ethereum developers:

- EVM Compatible - supporting generalized EVM smart contracts on a ZK rollup making it easy to deploy existing dApps
- ToolChain Compatible - able to port smart contracts with existing tools
- Ethos Compatible - aligned with the ethos of decentralization and open-source
- Certainty - using zero knowledge proofs offering certainty of security not probability
- Future Proof - ecosystem partners that adopt zkSync 2.0 now will enjoy all future improvements without the need to change their code

zkSync Era Mainnet was launched on March 24, 2023. zkSync currently crossed over $400M TVL (grown +50% in the last four months), and unique wallets have crossed 3.7M. Transaction volume has averaged +15% week-over-week growth the last four months with a few times surpassing Ethereum itself on daily transactions.

This marks just the beginning with key network infrastructure upgrades coming within the next few months which will catalyze growth of TVL, users and transaction growth, as many protocols will now be able to launch.

2. High Demand for wstETH:

Lido wstETH has the overwhelming market share of staked ETH and can be used interoperably in DeFi. Therefore, major ecosystems such as zkSync have significant demand for wstETH as it opens up opportunities for users to utilize stETH holdings in various DeFi protocols. Some examples include using wstETH as collateral, lending, farming, indexing, minting, vaults, stables, etc.

3. Implementation

TxFusion in collaboration with Matter Labs, undertook the initiative to design, implement and deploy the canonical wstETH bridge between Ethereum (L1) and zkSync (L2) networks. They have meticulously examined open-source solutions used for Optimism and Arbitrum, adapting the code to optimize for zkSync Era. The mainnet and testnet deployment addresses, along with audit reports, will be provided upon deployment. These details will be essential for the Lido DAO to assess the security and reliability of the bridge.

Technical Details

Lido wstETH bridge contracts have been designed with a focus on upgradability and they are owned by the Lido DAO on Ethereum. Consequently, no actions or modifications can be executed on the bridge without the explicit approval of the Lido DAO deployed on L1.

In order to bridge governance decisions from L1 to L2, TxFusion deployed the Governance bridge on L2 (ZkSyncBridgeExecutor) to facilitate trustless execution of arbitrary actions on L2 upon governance approval on Ethereum. This bridge represents the upgradeable version of AAVE cross-chain governance bridge adjusted to operate on zkSync Era.

As part of the solution, TxFusion developed and deployed the bridged wstETH token representation, following the ERC-20 standard. Furthermore, token implementation incorporates the support for ERC-2612 signed approvals (permits) and Smart Account signatures ERC-1271.

All contracts have been subjected to an audit conducted by Cantina (Spearbit), and the required improvements have been applied after initial review.

Emergency Brakes

For security reasons, it is recommended to set up multi-sigs on Ethereum and zkSync Era Mainnet which can disable deposits and withdrawals in case of an emergency. The multi-sigs can only disable deposits and withdrawals on their respective network. However, only the Lido Aragon Agent is capable of enabling bridge operations. The addresses will be finalized during mainnet deployment.

4. Ownership & Governance

The management of the bridge components is intrinsically linked to the Lido DAO. As such, we propose that the Lido DAO formally accepts ownership and control over the bridging parts. This will empower the Lido community to oversee and make decisions regarding the operation of the bridge, ensuring its alignment with the broader objectives of zkSync Era DeFi and the Lido ecosystem.

5. Next Steps

The relevant smart contract addresses and documentation will be made available after mainnet deployment. These details will be published and thoroughly documented to provide full transparency and accessibility to the Lido community. The community is encouraged to review the documentation and raise any questions or concerns before the Snapshot vote.

6. Conclusion

This proposal aims to formalize the ownership and control of the wstETH bridge on zkSync by the Lido DAO, thereby enabling the seamless integration of wstETH into the zkSync Era DeFi ecosystem. The bridge will play a pivotal role in supporting a vibrant and attractive DeFi space and will cater to the needs of various projects seeking to leverage wstETH. We invite the Lido community to engage in discussions and provide feedback as we move forward with this exciting development.

Audits

- Governance crosschain bridges (ZkSyncBridgeExecutor): TBD
- wstETH token bridge (L1ERC20TokenBridge, ERC20Bridged, L2ERC20TokenBridge): TBD

Testnet Contracts

- DAO Agent on L1: 0x4333218072D5d7008546737786663c38B4D561A4
- Emergancy Brakes Lido’s EOA: 0xa5F1d7D49F581136Cf6e58B32cBE9a2039C48bA1
- L1Executor: 0x3f33402FBbaE3e9Cf953e25F8b7D778342E67a77
- wstETH on L1: 0x589d420D66B7826DaC1158323EF1D2C42A2d1b08
- L1ERC20Bridge: 0xAd5c2a39eD9A8cB32A92E8510AECAF478222B565
- wstETH on L2: 0x948947F2f05864032Fb340E574D0F13C6BA7bE74
- L2ERC20Bridge: 0xaA040F9b7e1f1cEe8704e6D076ffD63410Acfd1E
- ZkSyncBridgeExecutor****: 0xfEF1a26853D2a4133017849f5738eaE92fb8117e

Mainnet Contracts

- DAO Agent on L1: 0x3e40D73EB977Dc6a537aF587D48316feE66E9C8c
- Emergency Brakes 3/5 Multisig on L1: 0x73b047fe6337183A454c5217241D780a932777bD
- Emergancy Brakes 3/5 Multisig on L2: 0x0D7F0A811978B3B62CbfF4EF6149B5909EAcfE94
- L1Executor: 0xFf7F4d05e3247374e86A3f7231A2Ed1CA63647F2
- wstETH on L1: 0x7f39C581F595B53c5cb19bD0b3f8dA6c935E2Ca0
- L1ERC20Bridge: 0x41527B2d03844dB6b0945f25702cB958b6d55989
- wstETH on L2: 0x703b52F2b28fEbcB60E1372858AF5b18849FE867
- L2ERC20Bridge: 0xE1D6A50E7101c8f8db77352897Ee3f1AC53f782B
- ZkSyncBridgeExecutor**: 0x139EE25DCad405d2a038E7A67f9ffdbf0f573f3c