Summary:

Composable IBC facilitates trust-minimized cross-ecosystem communication among various blockchains, including Polkadot, Kusama, Cosmos and soon Ethereum mainnet and Solana. This proposal outlines the integration of Composable for seamless and secure stETH bridging between blockchains. The Composable IBC protocol, as an extension of the Inter-Blockchain Communication Protocol (IBC), is a light client-based bridging framework which offers a trust-minimized solution for cross-ecosystem communication.

Introduction:

Composable IBC is an implementation of the existing IBC protocol, designed to bridge the gap between different blockchain ecosystems. While the original IBC protocol enabled trust-minimized bridging between Cosmos SDK chains, Composable IBC expands this capability to other ecosystems, including Ethereum and Solana. This proposal aims to address the challenges associated with existing bridge integrations, such as numerous assumptions and the need for trust in third-party intermediaries.

With discussion around multi-chain availability of stETH, we believe IBC should be brought into the discussion as it upholds key considerations around decentralization and security when moving tokens across chains.

- IBC provides a trustless and permissionless means for blockchains to communicate. They can exchange data, primarily tokens, without the need for direct communication between the chains. This decentralization and trustlessness are achieved through dedicated channels and smart contracts.
- IBC's trustless relayer mechanism ensures the security of data as it is sent via dedicated channels. It reduces the need for users to trust third-party bridges, enhancing the overall security of cross-chain interactions.

Secure and trustless bridging becomes paramount to token bridging in general, and highly critical to 'staked' assets such as stETH as these tokens underpin security in the asset's native chain. It is paramount to avoid potential pitfalls in bridging implementations such as the possibility of excessive minting of a token.

IBC Overview

The Inter-Blockchain Communication Protocol (IBC) is a protocol designed to facilitate the authentication and transportation of data between two blockchains. It operates with a minimal set of functions defined in the Interchain Standards (ICS). Importantly, IBC does not limit the network topology or consensus algorithm of the blockchains it connects, making it versatile and adaptable for use with a wide range of blockchains and state machines. The following features highlight key benefits to utilizing IBC:

i) Permissionless and Secure:

IBC offers a permissionless way to relay data packets between blockchains, unlike most trusted bridging technologies. The security of IBC relies on the security of the participating chains.

ii) Modularity and Composability:

IBC separates the transport layer (TAO) responsible for secure connections and data authentication from the application layer, which defines how data packets are packaged and interpreted. This modularity enables composability and the ability to design applications on top of IBC.

iii) Light Clients and Relayers:

IBC relies on light clients and relayers to ensure the validity of cross-chain transactions. Relayers are responsible for scanning the state of participating chains, constructing datagrams, and executing them on the receiving chain. Light clients efficiently verify the relevant state of the counterparty blockchain.

iv) Security:

IBC's security is based on trusting the consensus of the connected chains. It also implements fault isolation mechanisms to limit damage in case of malicious behavior.

Technical details of Composable IBC:

Before Ethereum shifted from Proof of Work (PoW) to Proof of Stake (PoS), creating a light client was a daunting task. PoW blockchains, including Ethereum, posed challenges like resource-intensive PoW validation, large storage requirements, slow syncing, and, most significantly, non-deterministic finality. This complexity made implementing light clients almost impossible compared to PoS blockchains.

Composable has made significant progress in developing light clients for networks that lacked them. This includes creating a

Casper light client for Ethereum's Beacon Chain, which will be deployed on the Composable Cosmos chain.

It is important to note that the Casper Light Client relies on the Sync Committee, providing an efficient way to verify Ethereum signatures.

Composable has implemented a Tendermint light client on Ethereum via a smart contract. This client verifies block headers from the Composable Cosmos chain and uses ZK-Snarks to verify signatures efficiently.

The goal is to make attacks more expensive than the combined market cap of DOT and ETH, although this may not cover all attack costs due to the limited slashing of validator bonds.

Other essential components include Hyperspace - an IBC compatible relayer, and an IBC implementation in Solidity. However, when extending IBC compatibility to Ethereum, it became imperative to supplement the relayer with a ZK-Circuit.

Challenges with Existing Bridge Integrations:

Existing bridge integrations often have numerous assumptions and dependencies on third-party trust and reliance on multisigs leading to potential security and reliability issues. In contrast, Composable IBC offers a trust-minimized approach to bridge different ecosystems, eliminating the need for third-party trust assumptions. This approach enhances the security and integrity of cross-ecosystem communication.

Security Considerations:

Composable IBC is designed to be trust-minimized and does not rely on third-party intermediaries or centralized control. This eliminates the potential risks associated with trust assumptions and enhances the overall security of cross-ecosystem bridging. Users can confidently transfer assets and data between different blockchains while maintaining control and security.

Timeline:

As of the current status, the Composable IBC bridge islive on Sepolia and Goerli. We are currently undergoing community testing and audits, which are expected to continue for approximately one month. Following successful testing, we plan to launch on Ethereum mainnet next month, providing a secure and reliable bridge for cross-ecosystem communication.

In summary, the integration of Composable Cosmos and Composable IBC offers a groundbreaking solution to the challenges of cross-ecosystem communication. By extending the capabilities of the IBC protocol, we provide a trust-minimised, secure, and efficient bridge for seamless asset and data transfers between various blockchains.

References

Composable Twitter / Discord -https://twitter.com/ComposableFin / Composable Finance

Ethereum IBC Ann. Blog -https://blog.cosmos.network/welcome-home-guide-to-participating-in-composables-ethereum-ibc-testnet-d1bf56a166ae

Ethereum IBC Testnet -https://app.trustless.zone/ethereum/

IBC Reference Information -https://tutorials.cosmos.network/academy/3-ibc/1-what-is-ibc.html