Hey everyone! Yorke and Jon here on behalf of Hyperlane to expand on an Eigenlayer middleware idea we are pursuing.

In this post we will introduce the Hyperlane interoperability protocol and demonstrate why its economic security model is an ideal launch partner for EigenLayer's Ethereum validator restaking initiative. We believe that collaborating would propel both ecosystems to new heights, bringing additional security to Hyperlane users and helping bootstrap demand for restakers.

What is Hyperlane?

Hyperlane is a smart contract protocol for simple and secure message passing between blockchains. This primitive enables interchain composability; examples include simple asset bridging, remote smart contract interaction, or multichain application architectures that leverage parallel blockspace or unique infrastructure features. Hyperlane's defining protocol characteristics are its modular security and permissionless deployment properties. Modular security, branded as [sovereign consensus,](#) allows developers to configure their own security model for each communication channel, potentially composing custom optimistic, proof-of-authority, or economic security models. Permissionless deployment means that Hyperlane can be deployed to any environment, chain agnostically, and enable interoperability with existing deployments.

Interchain Economic Security for Hyperlane

Because of its comparative latency and scaling benefits, economic security is one of the most compelling security models available to Hyperlane developers. A permissionless proof of stake system has validators stake on the source chain and sign outbound messages. If signatures commit to messages that were never sent, proof can be submitted on the source chain to slash the offending validators.

Unlike other interoperability systems with global validator sets and concentrated stake hub chains, Hyperlane validators stake on the same chain they are validating, ensuring that smart contracts can verify and slash for fraud without assuming any honest majority assumption. In exchange for this safety

slashing risk, validators are compensated by the protocol. There are no liveness requirements imposed on validators. With these slashing guarantees, message recipients can impose a floor on the economic cost to commit fraud before accepting a message, waiting for enough value at risk before proceeding with message processing.

EigenLayer Restaking for Hyperlane

The operational costs of a Hyperlane validator for a given chain come from the following requirements:

1. An event indexer, such as a tip syncing full node

2. A fixed-footprint datastore for making signatures available

The more significant prohibitive cost is the opportunity cost of capital for validators to stake.

Ethereum validators adding economic security to outbound Hyperlane messages is an ideal demonstration of the open innovation Eigenlayer can enable.

Safety violations are smart contract verifiable and because liveness is incentivized but not penalized, honest validators theoretically take on zero risk. Furthermore, the marginal cost of capital for eth2 validators to restake into Hyperlane is zero. Protocol fees distributed to Hyperlane validators serve as a strong incentive for validators to choose Eigenlayer as their staking provider.

Benefits to EigenLayer and Hyperlane

There is strong synergy and value alignment between the two protocols. Hyperlane becomes more useful because of the greater economic security, inducing more user activity and increasing fee revenue. For EigenLayer, demand from Hyperlane developers for additional security and additional revenue opportunities create demand to restake ETH. The Hyperlane protocol is in production and poised to bootstrap the market for restaked ETH and usher in the first set of paying customers.

We believe the two protocols are a great match for each other, and a relationship between the two will reinforce positive feedback loops for each of them.

Next Steps

We suggest that Hyperlane, in open collaboration with EigenLayer, integrate a Restaking Interchain Security Module for Hyperlane. This means that interchain application developers can secure messages from Ethereum using an Eigenlayer restaking set. Notably, it could be leveraged by new chains and rollups that have deployed Hyperlane themselves.

In continuing tradition of both teams, this integration would be developed in public as the Eigenlayer client and contract interfaces emerge. Lastly, we invite any and all feedback from the community and can answer questions from any interested parties of this joint offering of Hyperlane with augmented security by EigenLayer restaking in the thread.