Authors: Sora Suegami, Leona Hioki

TL;DR

We propose the concept of Octopus contracts, smart contracts that operate ciphertexts outside the blockchain. Octopus contracts can control the decryption of the ciphertexts based on on-chain conditions by requesting validators to sign the specified messages. Signature-based witness encryption (SWE) enables users to decrypt them with the signatures. Moreover, Octopus contracts can evaluate arbitrary functions on encrypted inputs with one-time programs (OTPs) built from SWE and garbled circuits. These features extend the functionality of smart contracts beyond the blockchain, providing practical solutions for unresolved problems such as a trustless bridge for a two-way peg between Bitcoin and Ethereum, private AMM, minimal anti-collusion infrastructure without a centralized operator, and achieving new applications such as private and unique human ID with proof of attribution, private computation with web data.

With Eigen Layer

There are several methods to select a validator set from the consensus layer of Ethereum as follows:

1. Hard fork Ethereum to force all validators to sign messages from Octopus contracts.

2. Soft fork Ethereum, allowing any validators to sign messages from Octopus contracts.

3. Use a re-staking mechanism such as Eigen Layer, enabling validators to have dual roles.

Even in the first case, which imposes the greatest burden on the Ethereum network, the validators' signatures for the same messages can be aggregated, so that the additional cost of pairing is at most for each ciphertext. However, in that case, we should note that security is not completely inherited because the validators cannot be penalized in the same way as in the case of double voting when they sign messages not specified by the Octopus contracts.

In the second and third cases, we can maintain the existing protocol of the consensus layer as the modification to the node implementation for our scheme is optimal in similar to MEV-related protocols.

Re-staking is the easiest way to achieve this architecture.

Read more

Full paper

Ethereum Research post