Below we provide some background on restaking and a potential centralization risk that may evolve specifically within Eigen Layer. To help mitigate this risk, we propose an Optimistic Delegation Framework. We do not think this solution is a silver bullet, but hope it inspires more discussion and solutions that may be implemented before this potential risk comes to fruition.

Background:

Restaking is a novel concept that enables the extension of existing trust networks to introduce new coordination mechanisms that they were not originally designed for. The restaking effort with the most mind share is currently Eigen Layer. While there has been debate across the Ethereum community around Eigen Layer, the team continues to ship and could be ready for applications built on Eigen Layer to start launching in 2024.

Challenge:

In Eigen Layer, each application / DApp will design its own actively validated services ("AVS") that will be run by "Operators". For some of these applications / DApps, the operational cost and complexity of performing the job and running the AVS may be minimal (referred to as "Lightweight AVSs" in the Eigen Layer white paper), however, in some instances the overhead may limit those who can perform the functions required by the AVSs (we refer to these as "Intensive AVSs")—limiting the Operator role to certain sophisticated participants. Due to this, Eigen Layer has created a "delegation framework" where those who don't want to, or more importantly can't, run the AVSs delegate their restaked ETH to an Operator. While this framework allows most Validators to participate in restaking, when Eigen Layer launches (and for some time), users can only delegate in an all or nothing relationship. Because of this design, there are economic incentives for solo validators to delegate (i.e., there is an opportunity cost to not running Intensive AVS), resulting in significant centralization of certain Operators. Eigen Layer's white paper proposed one solution called Hyperscale AVS to help alleviate this risk, which aims to reduce the load of an Intensive AVS (particularly for Eigen Layer DA).

Optimistic Delegation Framework ("ODF"):

The goal of this framework is to allow a Validator to directly participate in restaking by running AVSs, and not miss the opportunity to participate in Intensive AVSs. Similar to PBS in Ethereum, the goal of this framework is to separate the functions of heavy compute from the signature of a payload. To achieve this, we introduce a new participant referred to as the "Coprocessor" whose sole responsibility is to perform the complex functions required to support an AVS.

Description of framework:

- Validator wishing to restake their ETH downloads the Optimistic Delegation Framework software (this could be implemented via a few mechanisms, but below we'll refer to it as the "ODF AVS")

- Validator that is restaking then decides which AVSs they are comfortable running given the potential risks

- For the Lightweight AVSs, the Validator runs them as they normally would

- For the AVSs that are not lightweight, the ODF AVS allows for a Validator to select which Intensive AVSs they would like to opt into and receive bids from Coprocessors to perform the computational complexity required for Intensive AVSs

- Once a Coprocessor is selected, the Validator starts running the universe of selected AVSs (both Lightweight and Intensive AVSs) and when a signature is required for the Intensive AVSs, the Coprocessor provides a signature / proof and the payload to the Validator who signs the AVS as required by the network

- If the work is performed by the Coprocessor and signed by the Validator without slashing, the Validator shares some of the reward with the Coprocessor who performed the work

- If there is slashing, the Validator can submit a fraud proof and be compensated by the Coprocessor for the slashing of the Validator's restaked ETH. If the fraud proof is submitted, it does not delay finality of the network, just the reimbursement to Bob

[

ODF vf

1416×438 91.8 KB

](https://ethresear.ch/uploads/default/original/2X/f/fe0f042adf2a2b321a2e98b6a7e8606efddab546.jpeg)

We present a solution which can encode the varying levels of trusts. While an analogous system such as mev-boost currently relies on a fully trusted design, we present a solution which empowers the users of the protocol to change the level of trust by deciding the type and required amount of collateral / cryptographic approach.

Some near-term ideas to mitigate risk of Coprocessors not performing their role correctly:

- Restaked ETH: In the spirit of restaking, Coprocessors could be required to post restaked ETH to Validators

- Other Collateral: To act as a Coprocessor, collateral in another form could be posted that is commensurate with the restaked ETH at risk to slashing

- Reputation: Coprocessor stakes their reputation and are at risk of missing out on business opportunities if they fail to accurately perform the task required (we note that other challenges such as sybil resistance need to be thought about in this model)

- Cryptographic: While still a work in progress, there may be some ideas around cryptographic technics or hardware (i.e., TEE / MPC) that could reduce the collateral required to be posted / require no collateral be posted

This framework comes with trade-offs and open questions, which we attempt to capture below.

Pros:

- This framework could help reduce risk of centralization of operators and could allow for native restaking without delegation

- Similar to Ethereum, restakers can remain decentralized and enjoy associated economic benefits without the required overhead

- Restakers who want more specificity over which AVSs they are delegating to have the ability to trustlessly select the AVSs they opt into

- A thriving marketplace means healthy competition for Coprocessors and potentially better rates for restakers and reduces the risk of dominance of single Coprocessors as the compute / work required for an AVS may drastically vary

- The Coprocessor market could expand to a broader set of participants who may not be experts at running AVSs, but may be experts at the types of compute required

Cons / challenges:

- If collateral is required to be posted, there is a capital drag on Coprocessors

- This framework may drive further centralization of Coprocessors (this exists with or without the ODF) and if there is not enough Coprocessors bidding, we are stuck in the same centralized Operator market that would exist without the additional complexity the ODF may introduce

- Additional layers of middleware such as the ODF potentially increasing risk of slashing / having an impact on Eigen Layer / Consensus Layer of Ethereum

- While there are natural participants who may want to act as a Coprocessor, there is a cold start problem and a market for Coprocessors needs to develop

- There is potential risk of collusion by Coprocessors

Open Questions:

- There are many potential auction mechanisms that match the Validator with the coprocessor; we see this as open design space

- The relationship between the Coprocessor and Validator will shift drastically as the slashing conditions in restaking platforms evolves and the type of Intensive AVSs that will come to market become clearer

- There will need to be development around assuring Alice receives her payment for work

- It is not clear how an Eigen Layer "veto committee" who reverses / invokes slashing could impact this framework. While this likely comes from an extreme event, it should be not ignored

Last, we have not explored using the ODF beyond the goals stated above, but if a robust market of Coprocessors develops, one could imagine many more applications could leverage a framework where a less sophisticated user or application may wish to outsource computational complexity.

*Important Legal Information & Disclaimer *

are subject to change. No obligation is undertaken to update any information, data or material contained herein.