Migrated from research forum. Original author: shenoy

Diving into the world of Ethereum staking, there's a groundbreaking approach that changes how we handle security and trust: Distributed Validator Technology (DVT). Projects like Obol and SSV are leading this charge, offering new ways to manage Ethereum validators. Now, imagine applying this tech to EigenLayer. It's all about tackling a tricky issue where stakers and validators, despite being on the same team, sometimes find their goals misaligned. This problem, known as the principal-agent dilemma, can create vulnerabilities in the system.

[

image

750×506 69.5 KB

](https://canada1.discourse-cdn.com/flex028/uploads/eigenlayer/original/2X/f/ff2a9516fe8caa49ca483d08e6736c4910368c3a.jpeg)

By integrating DVT into EigenLayer AVS validation system, Supermeta Restaking aims to bridge this gap, ensuring AVS Operators act in the best interest of restakers. It's not just about enhancing security or slash resistance; we believe this will be a move towards making EigenLayer validation more democratic and resilient. This integration could signify a leap towards a more balanced, efficient, and trust-minimized restaking ecosystem that's robust and aligned with community values.

EigenLayer Operators Centralization Risk

In EigenLayer, there's a struggle between wanting to keep things spread out (decentralized) and having a few people in charge (centralized), especially because most people are just looking for bonus yield on top of Ethereum rewards. The system tries to let everyone share control, but it's tough when not many are willing to take on the job and would choose to delegate the responsibilities instead.

While EigenLayer encourages a decentralized approach to Operators, the reality is nuanced, with a tendency towards centralizing delegations among a few professional Operators. This dynamic, coupled with the inherent risk of slashing up to 50% of the delegated stake, prompts a cautious approach to delegation.

It creates a single point of failure, making the network more vulnerable to attacks or malfunctions. If these operators act against the network's interest or collude, it could lead to unfair practices or even manipulate AVS. Moreover, centralization contradicts the foundational ethos of blockchain—decentralization—which aims to distribute power among its users.

What could go wrong?

When solitary operators have too much control of an AVS, several things could go wrong. Firstly, slashing risks become pronounced in centralized setups due to the potential for mismanagement by a single entity controlling the validator. This concentration can lead to penalties imposed by EigenLayer for infractions like double-signing or downtime, where the delegator's entire stake might be at risk.

Single private key risk and collusion are also major concerns. With centralized operations, the handling of operator keys by limited parties increases the chances of key compromise through attacks or internal collusion. Such scenarios not only endanger the AVS, but also compromise the security of the delegated assets.

The opportunity for collusion extends beyond just key management. In a centralized framework, the parties in control can potentially manipulate decisions or orchestrate attacks without significant checks and balances, undermining the fairness and security of the network.

Lastly, the risk of a 51% attack on an AVS is heightened in centralized systems. If a single entity or a colluding group of Operators gains control over the majority of the AVS' validation power with the help of delegated user funds, they can alter an AVS' state to their benefit, broadcasting illegitimate transactions, which fundamentally breaches the integrity of the validated service. This risk is not merely theoretical; I have personally experienced such an instance during my involvement in the Steem ecosystem, where Tron took over the consensus through collusion, leading to significant disruption and controversy.

These risks underline the necessity for distributed approaches, and Distributed Validator Technology (DVT) is a viable solution for decentralizing Operator control and mitigating the vulnerabilities inherent in solitary Operators. By distributing the responsibilities and decision-making power across multiple parties, a decentralized Operator can achieve a higher degree of security, resilience, and trustworthiness.

Introducing SuperOperators

SuperOperators within the Supermeta Restaking network represent the first step towards a decentralized framework for EigenLayer Operators. They are essentially an EigenLayer Operator instance, however, instead of being powered by a single node, they are powered by a cluster of nodes, functioning together to offer a distributed validation service, which is more resilient to the typical issues faced by solitary Operators. This collaborative approach inherently diminishes the risks tied to solitary Operators, such as single points of failure, and decreases the likelihood of successful collusive attacks that could compromise the AVS.

[

image

1380×776 116 KB

](https://canada1.discourse-cdn.com/flex028/uploads/eigenlayer/original/2X/4/4ce3b81a0ed85ea225628a244ffa31370c1ec499.jpeg)

The Supermeta DVT Operator Cluster, the foundation of SuperOperators, is designed to enforce a robust level of security. By leveraging Distributed Validator Technology (DVT), a SuperOperator, which receives the delegation via EigenLayer, distributes the task of AVS validation across multiple nodes. This not only enhances security, but also ensures slash resistance as the SuperOperator remains operational even if one or several nodes encounter issues. The interconnectedness of these nodes means that an attack on one is not sufficient to bring down the network, thereby significantly increasing the cost and complexity of potential attacks.

Furthermore, the private key of SuperOperator is distributed among multiple nodes within the cluster. This decentralization of cryptographic keys ensures that no single node possesses complete key, enhancing the overall security and resilience of the SuperOperator framework.

Supermeta FluxCapacitor Middleware

Supermeta's FluxCapacitor middleware client helps orchestrate a SuperOperator cluster. At its core, FluxCapacitor serves as the primary architect of key distribution, a crucial step in the establishment of resilient and secure clusters for individual Actively Validated Services (AVS).

The process begins with FluxCapacitor distributing cryptographic keys across the network, laying the foundation for the creation of clusters tailored to specific AVS requirements. Each node within these clusters assumes a dual role, simultaneously running the FluxCapacitor middleware client and the designated AVS client. This operation ensures that nodes are equipped to participate effectively in the validation process.

FluxCapacitor's responsibilities extend far beyond key distribution. Before any data or transaction is deemed valid, FluxCapacitor coordinates the nodes to reach a consensus, thereby safeguarding the integrity and reliability of the network's validation mechanism.

The inclusion of FluxCapacitor's consensus mechanism adds an additional layer of security and trust to the EigenLayer ecosystem. By requiring nodes to agree on the validity of transactions before broadcasting them to the network, FluxCapacitor mitigates the risk of fraudulent or malicious activities, reinforcing the network's resilience against potential attacks.

Addressing the Principal-Agent Dilemma in AVS selection

EigenLayer currently employs a double opt-in method, wherein delegators lack the ability to specify which Autonomous Validation Service (AVS) their operator should opt into. This lack of transparency creates another opportunity for the principal-agent dilemma to emerge, where the interests of the delegator and the operator may not fully align.

We are working on a novel solution by incorporating a governance mechanism, where voting weights correspond to the delegation, empowering delegators to enforce the AVS their chosen SuperOperator will run.

Leveraging SuperOperators for Liquid Restaking Protocols

The majority of LRT protocols emerging today promote anti-slashing protection through insurance funds, however, delegating to a DVT-powered SuperOperator could emerge as a superior approach. SuperOperators also offer a simplified structure for decentralizing the delegation to multiple operators.

Consider an LRT protocol seeking to delegate user funds towards validation of 5 Actively Validated Services, and to have sufficient Operator risk diversification, the protocol may choose to delegate to 5 different Operators. In this scenario, due to the current constraints set by EigenLayer, each account within the protocol can only delegate to a single operator. Furthermore, given that one operator instance can only operate one AVS, this constraint increases the complexity even further, resulting in substantially increased gas fees.

TotalDelegations=Number of AVS ×Number of Operators per AVS

TotalDelegations= 5 AVS × 5 Operators = 25 delegations

Consequently, the protocol’s architecture becomes more complex, and its operational efficiency is impacted. This example underscores the need for a solution like SuperOperators within EigenLayer, which can streamline the delegation process and enhance the overall efficiency of LRT protocols.

TotalDelegations=5 AVS × 1 SuperOperator per AVS = 5 delegations

Supermeta Restaking therefore addresses the complexity arising from the need to maintain multiple accounts for delegating to individual operators, thereby reducing gas fees and enhancing operational efficiency.

As we wrap up our discussion on Supermeta Restaking’s role in EigenLayer, we’re grateful for the support and collaboration of top-tier validators like HashKey Cloud, Staking4All, Stakin, StakingCabin, BrightlyStake, P-Ops Team, Nodes Guru, DoubleTop, Girnaar Labs, Pier Two, and Safe & Steady Staking. Together, we are driving forward our mission to achieve decentralization and slash resistance in restaking.

As we look ahead, we’re excited about the possibilities that lie before us. We invite you to join us in this journey of exploration and innovation. Your insights and contributions are invaluable as we continue to shape the future of decentralized networks.

Email: [[email protected]

](/cdn-cgi/l/email-protection#3f58527f4c4a4f5a4d525a4b5e115956)

Website: Supermeta.fi

Twitter: x.com/supermetafi