FULL PDF REPORT · JULY 2024

Understanding EigenLayer

WEB3 citizen
YOUR INFINITE GARDEN GUIDE

Guide

Introduction

EigenLayer has positioned itself as a leading project in DeFi, infrastructure, and Ethereum as a whole. We began studying EigenLayer as a way to understand one of the biggest narratives in 2024.

From building common understanding of the project, to its growing hype, Mainnet Launch in early April, to continuously launching partnerships with multiple services, EigenLayer has grown massively in the last 6 months.

As 2024 progressed we found ourselves immersed in investigating all aspects of the EigenLayer ecosystem: Actively Validated Services, Liquid Restaking Protocols, emerging tooling as well as risks and use cases that appeared along the way. We even created a newsletter as a way to keep up.

This report is an attempt to summarize these efforts, diving into relevant developments of the EigenLayer Ecosystem. Understanding EigenLayer is meant to be read as a snapshot in time. Static in Q2 2024 but summarizing relevant aspects of the protocol.

You'll find two main sections:

1. Introduction to EigenLayer: an overview of restaking, and then diving into specifics of the protocol, its mechanisms and incentives.

2. EigenLayer Ecosystem: we zoom out into a more comprehensive view of use cases with EigenLayer and expand on some protocols developing.

We hope you find as much value in it as we did in researching it.

Introduction to EigenLayer

What is EigenLayer?

At its core, EigenLayer is a set of smart contracts that enables an open marketplace that allows stakers to opt-in to validating external software modules.

Staking is the medium by which Proof of Stake networks can reach decentralized consensus on which blocks to produce. Since the Merge, participants run software that participates in maintaining network data by depositing ETH – their "stake" – into the Ethereum protocol. Their stake validates smart contracts and transactions on Ethereum Beacon Chain. As described in “Staking is Data Validation, Not Investment”, stake permits the protocol to financially punish negligent or malicious participants.

In 2023, EigenLayer introduced a novel idea: pooled security via restaking.

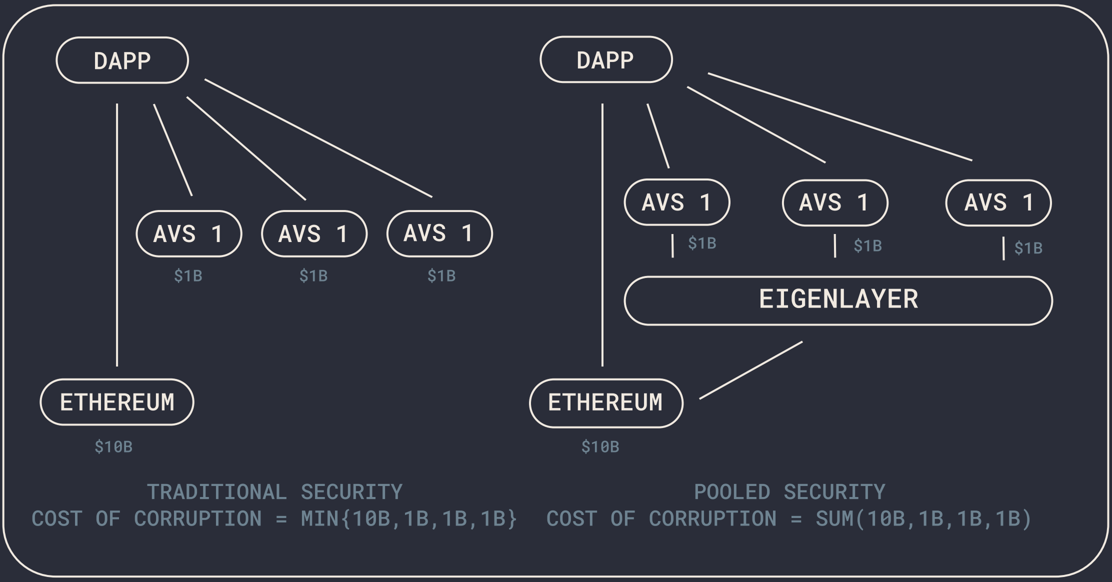
EigenLayer restaking involves stakers recommitting their stake to secure non-EVM transactions. Pooled Security via restaking refers to the mechanism that enables external modules to be secured by restaked ETH instead of being secured by their own tokens. The EigenLayer protocol pools that re-committed stake and enables the protocol to extend Ethereum's security beyond modules that are deployed or proven directly on top of the EVM.

Previously, dApps deployed on these modules relied on the protocol's security – which depended on their ability to bootstrap multiple validators to secure transactions. Now, modules can tap into Ethereum's network of decentralized trust, and the cost of corrupting a dApp depends on the amount restaked through EigenLayer.

> Protocols built on EigenLayer enjoy a Shared Security System, rather than building in fragmented security.

they can focus on protocol development rather than establishing a token and bootstrapping their own validator network.

Node Operators emerge as an intermediary, an entity or group of people that take on the responsibility of running client software and maintaining hardware. Similar to their role in Liquid Staking, Node Operators obtain delegated stake from stakers that opt into EigenLayer and restake it on their behalf.



COST OF CORRUPTING A DAPP INCREASES BY TAPPING INTO ETHEREUM'S SECURITY

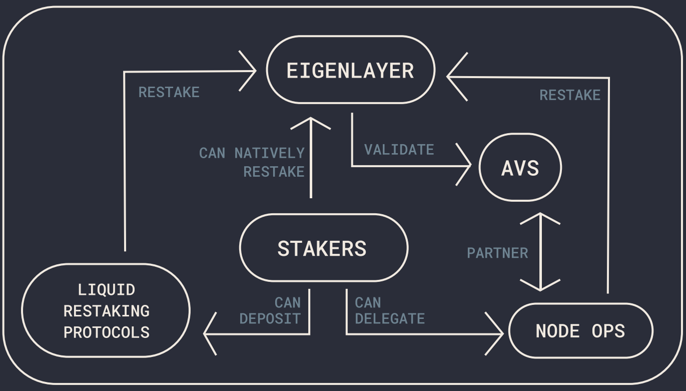
The second idea that constitutes the basis for EigenLayer is generating an open dual-side marketplace for that pooled security.

On one side of the marketplace, existing stakers agree and opt into validating additional modules, consenting to additional slashing risks. Through restaking, EigenLayer offers benefits to stakers as they gain additional rewards without much additional effort.

On the other side, external services such as oracles, ZK coprocessors, known as EigenLayer's Actively Validated Services (AVS) partner with EigenLayer to access pooled security for validating their transactions. Through restaking, they are supplied a way to get decentralized trust. This approach saves protocols a significant amount of time, as

For the EigenLayer marketplace to achieve high expressivity, it has to account for heterogeneity of its participants. This includes stakers who opt into the protocol but do not wish to run their own validators nor select their own node operators. Liquid Restaking Protocols provide a solution for pooled restaking, pooling funds from such stakers, partnering with professional node operators and restaking them on their behalf.

MARKETPLACE



Overview of Restaking

INTRODUCTION TO EIGENLAYER

Restaking with EigenLayer

Staking Paths

- **Solo-stake & natively restake**
- **Solo Stake & restake through:**
  - Liquid Restaking Protocol
  - Delegate to Node Operator
- **Stake through Liquid Staking Protocol & restake through:**
  - Deposit LST to Liquid Restaking Protocol
  - Delegate LST to Node Operator

All staking paths require choosing a validator to stake with. Stakers can either run their own validator securing Ethereum and natively restake with it, or delegate restaking responsibilities to a professional node operator.

Setting up a validator requires a significant amount of disposable capital, specifically 32 ETH, to deposit into the Ethereum protocol and activate a key-pair for signing off on the network's state. Running a validator also requires having technical knowledge, running all upgrades, upkeeping client software and ensuring validator liveness. However, if you already have a node, opting into restaking does not require much effort: downloading, running additional software, creating an EigenPod and reconfiguring the withdrawal address to point directly to the EigenLayer contract.

Within the EigenLayer contracts, EigenPods are smart contracts controlled by users that are designed to manage the balance and withdrawal statuses. Instead of a wallet being the withdrawal address, as with standard Ethereum solo-staking, stakers that opt into EigenLayer set their withdrawal credentials toward an EigenPod. The address that deploys an EigenPod becomes the sole owner of that Eigenpod contract and therefore gains permission for restaking and withdrawal operations.

EigenPods can serve as the withdrawal credentials for one or more Beacon Chain validators. Their role is to validate proofs for each of its validators.

Delegating stake to a node operator, on the other hand, is quite straightforward. You can select a Node Operator from EigenLayer's Marketplace of operators and delegate your LST or ETH. Otherwise you can deposit your LST of ETH into a Liquid Restaking Protocol (LRP). Each protocol works in partnership with various established Node Operators and manages restaking on behalf of depositors. By restaking with a LRP stakers point their withdrawal address to specific vaults or contracts owned by them.

Slashing

Slashing is a mechanism to secure and align participants within a network as it provides a way to impose economic penalties to those participants who behave in a way that diverges from what was specified within a protocol. It is unique to Proof-of-Stake networks, where participants deposit funds and agree upon conditions of a protocol's smart contracts.

Slashing is a key part in both Ethereum's and EigenLayer's incentive design.

In traditional Ethereum staking, dishonest behavior is incurred by validators when validators make attestations or block proposals that break specific protocol rules. Slashing events include signing two different blocks for the same slot, attesting to a block effectively changing block ordering or by attesting to two candidates for the same block ("double voting”). All of these cases are sufficient evidence of offenses and result in a slashing penalty to the offending validator. Validators are set to exit status and immediately lose a part of their stake (1/32 of their effective balance), missed epochs while in exit status, and additional penalties imposed. For more details on slashing penalties on Ethereum see The Eth2 Book.

Since withdrawal addresses are set within the EigenLayer contracts, EigenLayer can impose additional penalties for attributable, dishonest behavior by operators when validating AVS transactions.

Slashing presents an improved mechanism for the safety of a protocol since its imposed economic penalties increase the overall cost-of-corruption, that is to say the minimum cost of an adversary to mount an attack on a protocol.

Increasing the cost of corruption beyond what a malicious actor can retrieve from conducting an attack is effectively what makes a system safe, since there are no incentives for conducting said attack. As long as the cost of corruption is larger than the profit of corruption a system is considered to be cryptoeconomically safe. By using pooled security via restaking, EigenLayer increases the cost of corruption needed to corrupt AVS, while imposing additional slashing mechanisms that further increase that cost, maintaining security and deterring dishonest behavior.

EIGEN Token

INTRODUCTION TO EIGENLAYER

Introducing Cryptoeconomical Safety For Intersubjective Faults

In late April 2024, Eigen Labs introduced a limitation to restaking with the current EigenLayer model: it enables cryptoeconomical safety via slashing only for objective faults.

Objective faults are verifiable, can be attributed to some specific entity and can be verified objectively onchain. Examples of these can be double signing on a block. These types of actions can be penalized through slashing. In contrast, intersubjective faults are those faults that cannot be verified objectively onchain. These include claims about a blockchain on another blockchain (bridges), withholding data in the context of data availability and censoring transactions.

With the EIGEN token whitepaper, EigenLayer introduces a new method to induce cryptoeconomic penalties on intersubjective attributable faults committed by stakers.

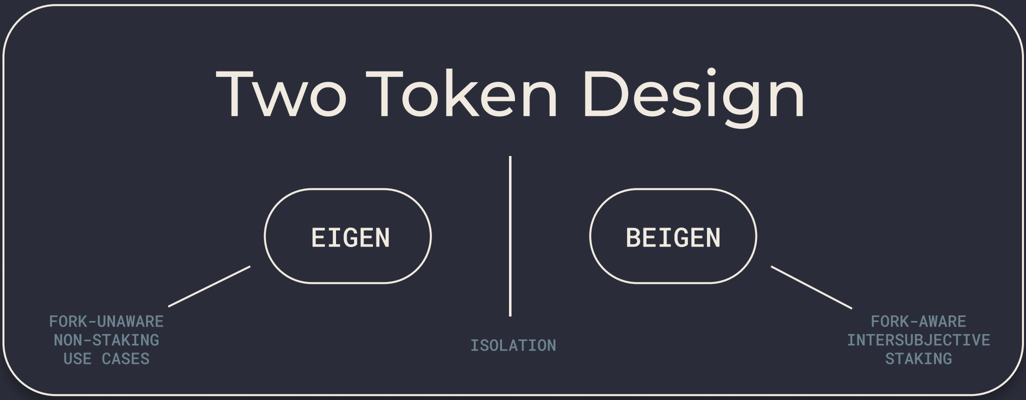
The EIGEN token would serve as a way to resolve disputes that cannot be identified on chain, but that can be agreed upon offchain. It does so by forking the token as a last-resort to resolve this issue.

However, the EIGEN token is inserted in a complex environment, where it can be used as a way to stake through EigenLayer, but can also be integrated into DeFi. The EIGEN model creates an isolation barrier between both use cases, allowing for a staked version of EIGEN to be aware of the forked state of the token, while another version can be unaware and locked in long term DeFi positions, among other non staking use cases.

In the event of a near-universal agreement on an issue, the fork-aware version of EIGEN would fork. Meanwhile, the fork-unaware bEIGEN will remain the same.

The EIGEN token unlocks the opportunity to solve problems that lie beyond what can be objectively observable onchain. This solution fully depends on the ability to arrive at a consensus on whether to choose a fork of a token, but does not require all users to keep up with the "true" EIGEN token.

TWO TOKEN MODEL ILLUSTRATION TAKEN FROM EIGEN: THE UNIVERSAL INTERSUBJECTIVE WORK TOKEN


Two Token Design
EIGEN
BEIGEN
FORK-UNAWARE NON-STAKING USE CASES
ISOLATION
FORK-AWARE INTERSUBJECTIVE STAKING

Benefits & Risks

INTRODUCTION TO EIGENLAYER

Benefits

EigenLayer provides incentives to all segments of the staking ecosystem.

EigenLayer's benefits

- **Pooled Security**
  Increases AVS Security
- **Attributable Security**
  Increases AVS Security
- **Flexibility to solve Intersubjective Faults**
- **Fosters ecosystem's innovation**
- **Network participation & decentralization**
- **Open marketplace**
  where participants express preferences

Pooled security increases AVS security

By leveraging pooled security, the EigenLayer protocol enables AVS to increase the cost of compromising their protocols from the minimum of the staked ETH in their individual networks to the sum of restaked ETH on EigenLayer. AVS built using EigenLayer tap into a shared security network and now share a base of security instead of only relying on their own token.

Besides benefiting from increased security, they benefit from reducing costs derived from the efforts to bootstrap their own validator set, establishing a token and monitoring security. Shared security enables protocols to focus on building and bettering their product.

Attributable security

The EigenLayer model of security establishes a way to increase the cost of corruption and slashing, which in turn increases the cryptoeconomic safety of a model. As defined in Stakesure, a model is cryptoeconomically safe if its cost of corruption is greater than the profit that any adversary can gain from an attack.

In Stakesure, EigenLayer explains a novel insurance model for AVS to ensure unconditional security, that is in the event of an attack no funds will be lost. This model is essentially an insurance model, wherein an AVS can buy security from EigenLayer to ensure that even if the protocol's service goes wrong no funds will be lost. This is attributable security and it could be given in addition to pooled security. Potentially, a marketplace for such attributable security could be created, depending on demand of said insurance.

This model is still in development. More info is introduced in Stakesure and the Columbia CryptoEconomics Workshop 2023.

Cryptoeconomical Safety For Intersubjective Faults

The EIGEN model not only includes a way to increase cryptoeconomical safety of protocols – slashing – and is open to guarantee attributable security through Stakesure.

With EIGEN, EigenLayer unlocks the opportunity to solve problems that lie beyond what can be objectively observable onchain. This solution allows for dual staking through EigenLayer (bEIGEN and ETH staking) and EIGEN integration into DeFi, but does not require all users to be aware of the "true" EIGEN token.

This allows for a better, more secure model to resolve disputes that ensure user/staker experience.

Fosters innovation

By reducing costs associated with building and creating an ecosystem with potential partnerships, EigenLayer lowers the entry barriers and facilitates agile innovation of protocols on top of Ethereum. Competing ideas can be implemented in a permissionless manner at a lower cost, without needing to bootstrap their own validators.

Increased participation & decentralization

An easy to grasp incentive for staker participation is, of course, increased revenue. Stakers accrue additional revenue streams with relatively low additional effort – especially if not native solo staker. Stakers can choose which modules and the amount of modules to secure. Additionally, they take on more risks by opting into additional slashing mechanisms for the modules they choose to validate.

In turn increased staker participation builds on Ethereum's and external protocols decentralization, while maintaining its security. Another feature we will not go in depth is the ability to delegate features for computational demanding tasks to allow participants without high-powered setups to pass on to those more equipped. This aims to reduce centralization in Ethereum given by computational demand, and ensures a greater participation in the network. Find additional information in the EigenLayer Whitepaper.

Creates an open marketplace

Within the EigenLayer marketplace, all actors, namely AVS, stakers and operators are able to achieve a high level of expression of their preferences. Stakers can choose among different staking paths, risk preferences. AVS can specify preferences in its contracts for the type of node operators or stakers participating in its validation when integrating with EigenLayer.

Additional Security Previsions & Risk Management

EigenLayer includes features to minimize the risk of unintentional slashing, attacks or any non objective protocol error. These include a mandated delay on unstaking. No matter the amount unstaked from EigenLayer smart contract, all withdrawals have a delay of 7 days needed for human monitoring in case of malicious action or attack on AVS.

EigenLayer designed a layer of governance to veto slashing decisions via multisig. The Community Multisig is composed of thirteen Ethereum aligned community members and is one of three multisigs in EigenLayer's governance architecture. The Community Multisig intervenes in case of a safety emergency, and it has the ability to veto slashing decisions. This is aimed at minimizing the chance of honest users getting slashed as a result of an unintentional slashing vulnerability, like a programming bug.

Risks

EigenLayer's risks emerge from actions enabled within its smart contracts. However, analyzing all risks is essential for a comprehensive view of the restaking risk landscape.

→ **Ecosystem Risks**
General risks associated with restaking

→ **EigenLayer Risks**
Specific risks that emerge from the protocol

Ecosystem Risks

Pressure on the Ethereum Protocol

A risk that emerges as the Ethereum ecosystem embraces staking and restaking during is the overload on messaging and aggregated signatures in the protocol. Currently, validators are operated with 32 ETH, a validators maximum effective balance and the amount of ETH that can earn rewards on. Large, professional node operators run multiple validators to maximize their staking rewards, and, as demand for staking services increases, so does the number of validators.

The proposed EIP 7251, also known as the Max EB proposal, could alleviate much of this network pressure if included in the Ethereum Pectra Network Upgrade. Max EB would allow large validators to consolidate their ETH into a single validator by increasing the maximum effective balance from 32 to 2048 ETH. This proposal also permits validators to earn rewards on any amount between 32 and 2048 ETH.

By incentivizing nodes to consolidate their stake, the proposal decreases the need for continually running more validators, thus reducing the pressure on messages and aggregated signatures. Additionally, it benefits solo stakers who have less capital than professional node operators. With the ability to compound rewards on amounts lower than 32 ETH, solo stakers wouldn't have to wait to reach 32 ETH to spin up a new validator, making the staking process more accessible.

Leveraged staking-restaking

On top of the earlier described restaking strategies, some stakers choose to increase the yield rewards on their staked assets using leveraged staking-restaking strategies. These stategies do not happen in the EigenLayer protocol and require an external lending market that integrates staking or restaking tokens.

For example placing an ETH deposit to stake on a Liquid Staking Protocol such as Lido, restaking the liquid staking token (i.e. stETH) on a Restaking Protocol receiving a liquid restaking token in return, then borrowing ETH on a lending protocol against that liquid restaking token to stake again.

Different combinations of staking, restaking, and borrowing on lending protocols and repeating that process can extract increased leveraged returns on the initial deposit. Highly leveraged stakers through lending markets are at risk of liquidations if the asset that is used as collateral depegs (i.e. the LRT depegs).

This exogenous risk is not a specific risk to EigenLayer since through EigenLayer, users cannot engage in any financial activities such as lending and borrowing. If a liquidation event occurs on a leveraged restaker, they lose their receipt token (LRT) and the liquidator simply buys it, assuming the staker's position and accrues any rewards from staking. It does not trigger any other cascading liquidation. It does, however, introduce a complex dynamic in the restaking ecosystem that other users should consider before financializing positions or when interacting with restaking protocols.

EigenLayer Risks

Slashing And Social Consensus

Even when actors are honest and well-intentioned, staking in multiple protocols simultaneously increases the chances of encountering bugs in the slashing contracts or client programs of these protocols, which could result in unintended slashing events. In a naive implementation of restaking, this could lead to a massive slashing event that undermines Ethereum's economic security. A potential solution could involve appealing to Ethereum's social consensus requesting the community to fork the chain, similar to the response to The DAO hack. In "Don't Overload Ethereum's Consensus," Vitalik argues against such a solution, explaining that it would be impractical for Ethereum to fork in support of various projects built on top of its economic security. Prioritizing larger protocols over smaller ones would stifle innovation and be detrimental to the ecosystem.

To prevent this, EigenLayer's slashing veto committee is entrusted with the power to veto unintended slashing events. Although this introduces a centralization point, it is crucial for preventing EigenLayer from jeopardizing Ethereum's consensus.

Delegation To Operators

When opting into restaking, EigenLayer allows stakers to delegate to node operators. The relationship between the staker and node operator is not guaranteed by the EigenLayer contract. Meaning, trust and quality service is not guaranteed because you can delegate to them. This introduces similar risks as those associated with traditional staking pools for Ethereum's Proof of Stake protocol, as stakers might choose a dishonest or underperforming operator, leading to reduced rewards and even slashing events.

When opting into restaking, EigenLayer allows stakers to delegate to node operators. The relationship between the staker and node operator is not guaranteed by the EigenLayer contract. Meaning, trust and quality service is not guaranteed because you can delegate to them. This introduces similar risks as those associated with traditional staking pools for Ethereum's Proof of Stake protocol, as stakers might choose a dishonest or underperforming operator, leading to reduced rewards and even slashing events.

Choosing a reliable operator is crucial, as users must trust that operators will perform their duties effectively and maintain high uptime. To mitigate risk, stakers can look into the operator's reputation and experience. Opting for reputable operators running nodes on hardware enclaves can also reduce dishonest behavior.

Additionally, centralization risks can emerge if a small number of operators accumulate a large portion of delegated stakes, undermining the decentralized nature of the network. To mitigate these risks, reputation systems or guides could be developed.

AVS Selection

Choosing which AVS to validate naturally involves certain risks. Even after undergoing smart contract auditing, there is still a possibility of encountering bugs and vulnerabilities in AVS codebases that could compromise the ecosystem's security and functionality. It is crucial for operators to analyze the reputation of an AVS before registering for them. EigenLayer and Eigen Labs put mechanisms in place to manage such risks, including the slashing veto committee.

EigenLayer Ecosystem

What to build in EigenLayer?

EigenLayer usecases stem from protocols that either can not be deployed or proven directly on top of the EVM or simply benefit from accessing Ethereum's trust network.

Protocols can be extremely specific or build various services within EigenLayer. These can be specialized on scaling Ethereum or extend and enrich the whole crypto ecosystem by enabling cross-chain use cases.

In cohesion with the rollup centric roadmap, EigenLayer enables various rollup services that add to the Ethereum rollup ecosystem. These include fast finality AVS, which create a layer where any rollup can assert and validate a rollup's state claim and attest its validity. Services such as AltLayer's MACH restaked rollups are already unlocking specialized fast finality layers for many rollups.

Another critical rollup service lies in Data Availability. Data Availability (DA) ensures that the necessary data for verifying a block is accessible to all network participants. Storing transaction data on the L1 chain, offers higher security but at a greater cost. EigenLayer can enable the extension of Ethereum's security while allowing Data Availability solutions, like EigenDA, to provide data storing services at a lower cost. Data-heavy consumer applications such as gaming can benefit from accessible, scalable and secure DA layers.

Sequencing establishes the order of events in the rollup, determining the order in which transactions will be processed in the rollup, creating transaction batches to submit to the L1 blockchain. Currently, rollups use centralized sequencers allowing for potential transaction censoring, manipulating transaction order, and even delay transactions. EigenLayer can unlock decentralized trust for protocols building sequencing services. Protocols such as Espresso's sequencing marketplace are already paving the way.

EigenLayer is also being leveraged by protocols in the applied cryptography space. Protocols are creating robust security systems using multiparty computation, Trusted Execution Environments (TEEs) to enhance transaction reliability and privacy, and Fully Homomorphic Encryption (FHE) to support encrypted computation.

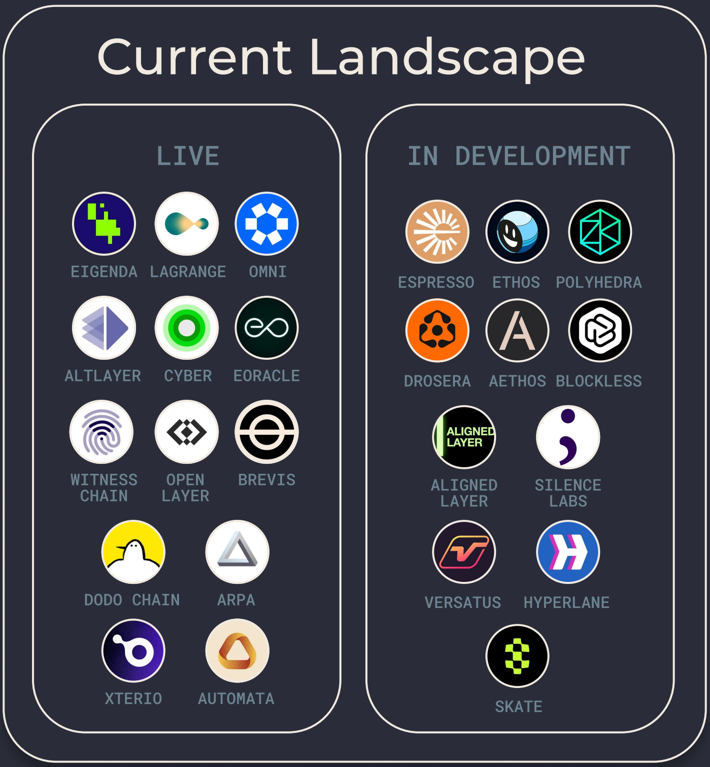
Even more use cases that emerge in the EigenLayer ecosystem are:

- Prover Networks and Relay Networks.
- Cryptoeconomic coprocessors, attaching integrity to claims.
- Verifying ZK proofs offchain and other proofs.
- Interfaces to securely interact with machine learning models or trigger computation secure transactions.
- MEV management applications, allowing proposers to make additional credible commitments on block inclusion and ordering
- AVS tooling, facilitating interactions between protocols.

You can find more use cases through EigenLayer's Ideas for Building the Next 15 Unicorns and Sreeram Kannan's interview on the Unchained Podcast.

AVS Landscape

During Q1 we have seen many projects launch implementations of these use cases.



We will dive into three key projects building in EigenLayer. This is not an exhaustive list, but rather a "jump-start" point to learn about AVS.

EigenDA

EigenDA was the first AVS on Mainnet. It stands as a secure, high-throughput, and decentralized data availability service built by EigenLabs.

While the rollup centric roadmap relies on rollups to take on some of L1's computation and execution load, scaling beyond the constraints of data availability and increasing throughput remains a challenge.

Ethereum has a fixed block size and gas limit which restricts the amount of data that can be included in each block. This can put a limit on the number of transactions (and the amount of data) that can be processed per second. As demand rises, data availability costs increase and the network's throughput is limited.

EigenDA proposes a model for DA, where data can be moved off-chain avoiding transaction data being sent and replicated to every node. Instead, only DA metadata and accountability processes are processed on-chain. This enables the DA architecture to scale horizontally with respect to the operator set. Currently, the protocol is running with 10 MB/s of write throughput, which is an order of magnitude improvement on current L1 DA rates after the Dencun Upgrade, and estimated DA rates after implementation of Danksharding.

Increasing scalability to data availability brings costs down. EigenDA helps with that, while leveraging decentralized trust through EigenLayer and ensuring a high composability and easy integration with rollups and apps. Overall, this model has the potential to significantly reduce the costs of innovating on Ethereum.

Find more information through EigenDA Docs and Awesome AVS.

Lagrange

Lagrange's mission is to enable large-scale verifiable computation over blockchain data using its hyper-parallel ZK Coprocessors. It focuses on three core projects: their ZK Coprocessor, Lagrange State Committees (LSC), an app on this coprocessor built as an AVS, and it's ZK Prover Network, a second app built as an AVS.

Lagrange State Committees

Lagrange State Committees are ZK light client protocols for optimistic rollups.

These committees are conceptually similar to Ethereum’s Sync Committee and support light client-based applications, such as bridges and interchain message layers, that use an optimistic rollup’s state without taking on excessive trust assumptions.

Each Lagrange State Committee is a decentralized network of nodes that have restaked 32 ETH as collateral via EigenLayer. Its network of restaked nodes attest to the finality of blocks within an optimistic rollup. These attestations are then used to generate state proof – cryptographic proofs of the blockchain’s state. These state proofs are useful for cross-chain applications as they prove the "true" state of that rollup. Lagrange's state proofs are verified by protocols including LayerZero, Axelar, and Polymer Labs.

State Committees are not designed to replace proofs of consensus but are an alternative mechanism for chains whose finality or consensus is not provable within a ZK context.

Key unlocks:

- **Shared Security:** LSC allows multiple cross-chain protocols to derive security from a single set of validators.
- **Scalability:** Each LSC network supports an unbounded set of nodes, bringing increased scalability.

It currently supports Base, Arbitrum and Optimism, but it's designed to be extensible to generate state proofs for any chain, using different consensus mechanisms or sequencers.

Implementation of LSC results in a secure fast finality hub for messaging and bridges, increased security for interoperability protocols and reduced overhead for teams building cross-chain products, as they can rely on LSCs network of restaked nodes for security.

Lagrange ZK Prover Network

Lagrange’s second AVS is the first production-ready zero knowledge prover network deployed in the industry.

A ZK prover network is a decentralized network designed to generate zero-knowledge proofs (ZK proofs) for various computational tasks. Lagrange's Prover Network provides ZK proofs while also creating a granular two sided marketplace where complex queries are met with predictable proof categorization and generation.

The network consists of two primary actors: Gateways and Provers. Each Gateway is connected to Provers in the network, and is responsible for managing a queue of work that different provers commit to perform. The first gateway, deployed by Lagrange Labs, powers Lagrange's ZK Coprocessor.

Operators run provers committing to generating proofs within a given time period by submitting collateral and agreeing to penalties if they don't comply with their tasks. Their assigned tasks are based on the amount of work they're able to process, as defined by their stake.

Benefits of this AVS include:

- High Liveness: By penalizing operator delays, the network ensures reliability and timely proof generation.
- It unlocks a larger scale of computational tasks and faster proving times, as it leverages many provers given by operators within EigenLayer that opt into this AVS.
- Highly scalable architecture: The prover network can scale as more provers (operators) join.
- Granular Proving Marketplace: Operators can choose to generate different types of proofs based on various requirements, creating a two-sided marketplace.
- Increases accessibility to ZK technology, enabling developers to integrate and utilize it in their applications.

Espresso

A sequencer's role involves collecting transactions, determining transaction inclusion and order, and settling them on Ethereum. In a decentralized sequencer, multiple servers are in charge of sequencing tasks. Shared sequencing allows many rollups to share a common mechanism or protocol to determine ordering of transactions.

Espresso is creating a marketplace for shared sequencing.

Espresso's marketplace will enable rollups to sell sequencing timeslots to sequencers (or shared proposers) through a combinatorial lottery – also known as combinatorial proposal selection, a mechanism to assign proposers to namespaces that is still under development. When a sequencer buys a timeslot, it gains the right to propose blocks for that rollup during that time slot. Additionally, Espresso's design will allow for L1 proposers to hold right of first refusal for the sale of any namespace proposing rights, giving them the option to purchase the rights from the assigned proposer.

HotShot is Espresso's consensus protocol. It offers high throughput and near instant finality, while being able to scale to a large number of participating nodes. As these participating nodes do not execute transactions, individual nodes do not need to access all the data, significantly reducing the hardware requirements to node participation.

Espresso's HotShot consensus separates DA and execution (which still happens at the rollup level) from consensus. For data availability, it relies on the Tiramisu DA layer, which ensures DA is available to all nodes participating in the network and supports HotShot's high performance.

Benefits of Espresso include:

- Sequencing transactions together can ensure atomicity of transaction inclusion across rollups.
- Increased fast-finality and reduced consensus communication complexity with the use of HotShot, retaining high security.
- Separation of DA from consensus using Tiramisu, enabling higher performance by processing more data.
- Optimistically responsive HotShot, committing new blocks as quickly as the network allows under favorable conditions.
- Increased modularity.

Espresso is not live on EigenLayer. For information on AVS and AVS tooling we recommend you also refer to app.eigenlayer.xyz and Awesome AVS.

Final Thoughts

You've reached the end of Understanding EigenLayer.

This report summarizes implementations, benefits, and risks within the EigenLayer model up until Q2 2024. We've covered the protocol's use cases and some of the many innovative projects being developed. Q3 will come with new AVS launches, developments in the dual staking model – which we have not covered in this report –, full availability of slashing and unlocking other features of the EigenLayer model.

We believe restaking can continue unlocking innovation and growing the infinite garden.

We look forward to the exciting innovations the second half of the year will bring. Onward!

How Can You Stay Updated

Throughout our research we created two initiatives:

- **EigenLayer News**: A weekly newsletter summarizing news and events in the EigenLayer Ecosystem.
- **EigenLayer Hub**: A hub with key resources, docs and guides on EigenLayer.

Feel free to reach out and give us your feedback!

Glossary

A - L

Actively Validated Service or AVS: An external protocol that leverages EigenLayer restaking to access pooled security to validate their transactions.

Beacon Chain: The main component of Ethereum 2.0, a proof-of-stake blockchain that manages the protocol and all of the shard chains. More details.

Coprocessor: Specialized processors with architectures dedicated to particular tasks with the aim of offloading heavy computation and enhancing performance.

Cost-of-corruption (COC): The minimum cost of an adversary to mount an attack on a protocol.

Cryptoeconomic safety: In the context of EigenLayer, a cryptoeconomic safe system is one where the cost of corruption is greater than the profit of corruption.

Danksharding: A proposal to increase Ethereum's scalability by expanding data blobs attached to Ethereum's blocks. Proto-Danksharding, brought by implementation of EIP 4844, is one of the many updates to realize Danksharding. It introduced data blobs that can be sent and attached to blocks. More details.

Data Availability (DA): Refers to the guarantee that the data needed to verify a block in the blockchain is available to all network participants.

Dencun: The Cancun-Deneb upgraded the Ethereum network in March 2024 to implement EIP 4844. See Danksharding.

Eigenpods: Smart contracts within the EigenLayer protocol controlled by users that are designed to manage the balance and withdrawal statuses.

EIP: An Ethereum Improvement Proposal updates Ethereum's contracts

Leveraged staking: A strategy used to increase staking revenue that involves using borrowed funds to increase the amount of staking tokens the user holds. This strategy involves a higher level of risk, as the asset (i.e. ETH) is borrowed against another asset whose price may vary.

Light client: In contrast to full nodes, a light client doesn't download or validate any transactions. They only download the block header, and assume that the block only contains valid transactions.

Liquidations: A process of converting assets, such as leveraged positions or collateral, into cash. It is usually triggered by unfavorable market movements, where the assets' value drops significantly.

Glossary

L-S

Liquid Restaking Protocols: Service providers that allow users to participate in restaking by depositing LSTs or ETH.

Liquid Staking Tokens (LST): Receipt token given to a staker on liquid staking protocols after locking their stake in a Liquid Restaking Protocol. Can be used to interact with other protocols, such as DeFi or Liquid Restaking Protocols

Liquid Staking Protocols: Service providers that allow users to participate in Ethereum Consensus. They facilitate staking for those users who either lack 32 ETH or want to delegate responsibilities of management.

Maximum Effective Balance: The effective Balance of a validator represents a value calculated by the current balance. It is used to determine the size of a reward or penalty a validator receives. Currently, the Maximum Effective Balance of a validator is 32 ETH. More details.

Maximal Extractable Value or MEV: Refers to the maximum potential profit a miner or a network participant can extract from block production and transaction ordering.

Node Operators: Entity or group of people that take on the responsibility of running client software and maintaining hardware. In the context of EigenLayer restaking, operators receive delegated stake from stakers and validate AVS.

Pectra: The Prague-Electra is the next Ethereum Network Update, scheduled for early 2025. More details.

Restaking: A mechanism that involves stakers recommitting their stake to secure non-EVM transactions.

Sequencing: Refers to a Sequencer's tasks: collecting transactions, determining transaction inclusion and order, and posting them on Ethereum.

Shared Sequencing: A sequencing design wherein many rollups can share a common sequencer, achieving greater interoperability.

Slashing: a mechanism to secure and align participants within a proof-of-stake network. It provides a way to impose economic penalties to those participants who diverge from what was specified within a protocol.

Staking: To validate transactions and create blocks, proof-of-stake blockchains require participants to lock up a certain amount of funds to act as collateral. Staking is the action of depositing funds required to participate in validation.

Glossary

S-Z

State Proofs: Refer to cryptographic proofs of the “true” state of a blockchain.

V**alidators:** An entity on the Beacon Chain, represented by a balance, public key, and other properties, that participates in consensus of the Ethereum network.

Validator Client: The software that acts on behalf of the validator by holding and using its private key to make attestations about the state of the chain. A single validator client can hold many key pairs, controlling many validators.

Zero-knowledge proof: A method by which one party (the prover) can prove to another party that a statement is true, without revealing to the verifier any information beyond the statement's truth.

Thanks!

FIND MORE @

X.COM/WEB3CITIZEN

HELLO@WEB3CITIZEN.XYZ

WWW.WEB3CITIZEN.XYZ