Risk FAQ

General Questions

Is EigenLayer a DeFi protocol?

No, EigenLayer is not a DeFi protocol. EigenLayer is a platform to bootstrap new proof of stake (PoS) systems. Through the EigenLayer protocol, users CANNOT engage in any financial activities such as swapping and lending.

However, for the decentralized services built on top of EigenLayer (we call them AVSs, Actively Validated Services), these services could be DeFi applications themselves or support key functionalities in other DeFi protocols. These AVSs are external to the EigenLayer contracts.

Moreover, another class of protocols built on top of EigenLayer is called liquid restaking protocols (LRT). They are permissionlessly built on EigenLayer. We urge users to do their own research before interacting with LRTs.

Does EigenLayer reuse the same economic security?

Yes, EigenLayer does reuse the same economic security by enabling different AVSs to share a common economic security base. This concept is known as 'pooled security.' Similar to how various dApps share Ethereum's economic security, EigenLayer allows different decentralized PoS networks share the same economic security base.

Pooling allows various AVSs to contribute to a larger, shared economic security base, enhancing economic safety. This is because the cost to compromise any individual AVS increases significantly. For instance, consider 100 AVSs each with 1B in economic security versus 100 AVSs sharing 100B in economic security. The cost to attack any single AVS in the pooled system has effectively multiplied by 100.

In addition to pooled security, EigenLayer will let each AVS acquire additional attributable security. Unlike pooled security, attributable security is specific to each AVS and will only be slashable by one AVS. This arrangement can provide game-theoretic guarantees for AVS customers.

Imagine a bridge protocol with a shared security base of 10B and an attributable portion of 10B. If a malfunction occurs, the protocol can assure the AVS customer that up to 10B can still be securing the bridge through the attributable part. Attributable security also enables the flexible scaling of economic security. As an AVS, you can adjust your security budget based on user demand, catering to varying user needs at different times.

Furthermore, EigenLayer aims to achieve economies of scale by allowing AVSs to share the same underlying smart contract infrastructure. If a DeFi application uses services from five different AVSs and requests 100B in economic security, these AVSs can collectively purchase attributable security instead of each buying 100B individually. This is feasible because if any of them fail, the 100B could be compensated to the DeFi protocol.

In conclusion, EigenLayer will not only allow AVSs to share economic security but will also enable individual AVSs to acquire additional attributable security. The combination of pooled and attributable security allows EigenLayer to flexibly and efficiently scale economic security.

Why is EigenLayer's contract licensed under BSL?

EigenLayer's core contract operates under BSL due to the numerous market forces at play. EigenLayer is not isolated; it operates within a broader ecosystem. Innovators can utilize the comprehensive decentralized trust network of the Ethereum economy with EigenLayer, eliminating the need for new token creation.

Without the need for a new token, this makes it easy for other entities, particularly those with extensive product distribution, to replicate and utilize the code. This situation applies to AVS building on EigenLayer and EigenLayer itself.

In scenarios where major LSTs have a much larger distribution and no new token is required for new networks, it becomes crucial to establish boundaries to safeguard open innovation. This protection ensures that individual LSTs do not consume open innovation and that existing protocols are not easily copying AVS designs. Consequently, EigenLayer's core operates under the BSL, transitioning to the MIT (Massachusetts Institute of Technology) license after two years, a practice also followed by some AVSs.

We are also exploring new licensing models that combine the benefits of protected licensing, which ensures value accumulation for innovators with permissionless innovation, which allows the creation of derivatives without needing explicit permission. Until we finalize these new models, we will continue using the tried-and-tested BSL model. If Ethereum core developers express an interest in enshrining EigenLayer before the BSL expires, we are more than open to collaboration as well.

Staker Related

Is EigenLayer rehypothecating my staked tokens?

No, EigenLayer does not engage in rehypothecation.

Rehypothecation is the practice that allows collateral posted by, say, a hedge fund to its prime broker to be used again as collateral by thatprime broker for its own funding.

Rehypothecation in traditional finance implies:

1. Depositor no longer have direct control of their assets.
2. Depositors have little say in the financial activities conducted by the intermediary.
3. Depositors are subject to substantial liquidity and counterparty risks.

Whereas in EigenLayer:

1. Stakers retain full control over their staked tokens.
2. Stakers have autonomy over the services they wish to validate.
3. Stakers are not exposed to counterparty liquidity risks.

There are clear differences between EigenLayer and rehypothecation.

AVS Related

Doesn't EigenLayer remove all the utility from an AVS network token?

No, EigenLayer doesn't remove the value of any hypothetical AVS tokens, but adds more value to it.

Firstly, Ethereum's L2 networks serve as a greatest counterpoint to this line of logic. Despite outsourcing their network security to Ethereum, L2 tokens maintain significant value within their respective networks.

Secondly, if an individual AVS decides to incorporate its own token for staking and network operations, EigenLayer supports [dual staking](#) . In this setup, an AVS can be secured by two types of assets, likely one in ETH and one in its native token.

It's important to note that in the dual staking model, AVS governance always has the ability to adjust the balance between AVS's native token and ETH within its network.

During the initial phase, an AVS may choose to rely more heavily on ETH, giving it greater weight to mitigate the inherent risk of relying solely on its native token, which could potentially lead to a downward spiral. However, as the AVS matures and gains more adoption, the governance can adjust the balance to give more weight to the AVS token, thereby increasing its value.

These points provide individual AVS with more options than the current status quo. Building on EigenLayer, therefore, doesn't negate the utility of an AVS token. Instead, through these additional options, we enhance their value.

Given the answer above, does it mean EigenLayer provides little value beyond the bootstrapping phase?

No, EigenLayer offers significant value at any stage of the AVS's economic security phase.

Firstly, the use of ETH as the shared security set inherently reduces the endogenous risk associated with a native AVS token.

Secondly, as the AVS ecosystem matures, interoperability between different AVSs and the resulting synergy will become a crucial factor enabling AVSs to leverage EigenLayer.

Thirdly, the flexible security that EigenLayer provides proves beneficial in handling security demand shocks for AVSs. If an AVS needs to secure a large customer transaction suddenly, it can quickly access the necessary security.

Finally, building on the synergy point, as AVSs begin to serve more customers collectively, the economic scale of insurance will enable AVSs to meet their customers' need for cryptoeconomic security more affordably.

LRT Related

What roles does LRTs serve?

LRTs safeguard EigenLayer and AVSs from external financial risks tied to staked positions. In EigenLayer, stakers don't receive a transferable receipt post-staking. Despite this, we expect some stakers to try and financialize their positions.

In the absence of LRTs, if a financialized staker's position gets liquidated, the staked tokens must be withdrawn from EigenLayer. This is the case because staked position cannot be transferred, negatively affecting AVS's economic security. However, with LRTs, withdrawals become unnecessary. The liquidator can simply assume the staker's position.

This feature is especially crucial during substantial market downturns. As the price of ETH falls, so does the system's total economic security. If liquidation leads to more ETH leaving EigenLayer, it would worsen the downward spiral. LRTs can significantly mitigate this risk, thereby protecting both AVS and EigenLayer from potential financial risks related to staker positions.

Is there an LRT looping risk that would potentially cause potential liquidation cascade?

No, looping LRTs in EigenLayer is not possible because depositing LRTs into EigenLayer is currently not allowed.

However, in lending markets, looping LRTs may occur based on the risk analysis of individual LRTs. We advise caution when taking this step as it involves financial leverage and exposes LRT holders to significant risks.

Looping LRTs in lending markets can lead to a cascade of liquidations. This risk is limited to individual lending markets and does not affect the security of EigenLayer. This is similar to the stETH depeg incident in 2022. During the event, the price risk of stETH is contained within the lending market, and Ethereum consensus remains unaffected.

Ethereum Related

Does EigenLayer rely on Ethereum social consensus?

No, EigenLayer does not depend on Ethereum's social consensus. EigenLayer aims for responsible decentralization. Instead of shifting unwarranted slashing risks to Ethereum or external protocols, EigenLayer includes a slashing veto committee. This internalizes social consensus and safeguards against slashing risks.

The veto committee functions similarly to the relay in MEV-Boost. MEV-Boost relies on a double-trusted party, known as a relay, who is trusted by both proposers and builders. Any individual trusted by both parties can serve as a relay, effectively removing any entrenched actor.

In EigenLayer, a veto committee will serve as a doubly-trusted intermediary between AVS and staker. The solution is the same as the relay, but instead of having a specific veto committee, anyone will be able to establish a veto committee. As long as both parties trust the committee, the staker and AVS can interact through it.

The intention is to upgrade to a version of EigenLayer without a canonical veto committee. Instead, there will be a marketplace of veto committees. Operators and AVSs would both be able to define their veto committee preference. AVSs and Operator veto committee choices would need to overlap in order for an operator to opt in to an AVS. This promotes inter-subjectivity, as operators and AVSs coordinate their choices based on their subjective views of safety.

Does EigenLayer increase centralization pressure on the validator set?

If EigenLayer imposes additional computational demands on Ethereum validators, it unavoidably becomes a centralization vector for Ethereum. With this principle in mind, EigenLayer discourages the increase in node requirements for Ethereum validators and promotes the use of lightweight AVSs, such as EigenDA .

For more computationally demanding AVSs, EigenLayer's delegation features allow Home stakers to secure Ethereum while delegating the operation of other AVSs to a different operator.

Ongoing research is focused on mechanisms, such as the Optimistic Delegation Framework and [AVS for PBS](AVS for PBS) , to reduce the computational load on Ethereum validators in a trust-minimized manner.

From an economic standpoint, we are exploring the possibility of directly incentivizing individual stakers through a rewards sharing scheme. Consider, for instance, allocating a certain percentage (x%) of all rewards processed through EigenLayer to solo validators.

If you are interested in discussing these mechanisms and incentive issues further, please share your thoughts on research.eigenlayer.xyz

Does EigenLayer eat away into the security margin of Ethereum?

No, EigenLayer does not compromise Ethereum's security margin.

When the stake in EigenLayer is significantly less than the total staked ETH, it does not impact Ethereum's security.

If the stake in EigenLayer makes up a large part of the total staked ETH, EigenLayer doesn't put the entire stake at risk. Instead, it sets aside a portion as a buffer for Ethereum, offering only the remaining stake for security. This approach ensures that we can consistently safeguard Ethereum's security margin.

For a better understanding of the required security level for Ethereum, we suggest readers refer to StakeSure .

Does EigenLayer need to self-limit like other liquid staking protocols?

No, EigenLayer doesn't require self-limiting.

The danger of a liquid staking protocol owning a substantial portion of the network is the potential imposition of a specific validator set on the Ethereum network. This risk doesn't apply to EigenLayer. Even if all staked ETH is restaked through EigenLayer, it doesn't control Ethereum's validator set. That control remains solely with Ethereum's stakers and validators.

If EigenLayer self-limits, the surplus restaking demand will likely revert to liquid staking protocols, increasing centralization pressure at the protocol's base layer. If EigenLayer didn't exist, dominant LST protocols would likely offer restaking services only to their internal stakers. These centralized restaking services could considerably strengthen the dominant LST's central position. More restaking services mean additional yield, leading to further consolidation of the LST. This scenario resembles the situation with MEV, where large stakers, including professional operators and LSTs, can negotiate MEV order flow guarantees that smaller stakers can't participate in.

In contrast to the centralized restaking mechanisms mentioned above, EigenLayer is developing a credibly neutral, decentralized restaking platform. All participants, whether small or large LSTs, small or large node operators, or institutional and home stakers, can all participate in additional validation opportunities. This approach helps prevent a monopoly in LST or LRT, fostering decentralization and neutrality among node operators.

EigenLayer doesn't define an operator set, so it doesn't threaten Ethereum's censorship resistance or operator decentralization.

Self-limiting EigenLayer offers no significant benefit. Instead, if EigenLayer proves successful in the market, it could even be integrated into the Ethereum protocol as a native service.

Does EigenLayer experience the principal-agent problem between stakers and operators?

EigenLayer, as with other PoS protocols, does experience the principal-agent problem. However, our goal is to minimize this issue as much as possible.

It's important to highlight that EigenLayer operators never retain custody of the staker's tokens, which limits the potential for malicious activities to only slashing events.

We have established several strategies to further limit the operator's capacity for harmful actions:

1. Technical Trust: EigenLayer operators can utilize an anti-slasher within a Trusted Execution Environment (TEE) to verify its response to any validation task. The operator then sends the associated TEE certificate with its response for the task, confirming that the anti-slasher was utilized. Another technical solution to address the principal-agent problem is to structure the EigenLayer operator with decentralized DVT nodes.
2. Economic Trust: Similar to RocketPool, a specific LRT protocol might require operators to stake proportionally to the delegation they receive. This approach assumes a certain amount that can be slashed and a probability for that occurrence. By encouraging the operator nodes to behave correctly, the principal-agent problem can be mitigated.
3. Social Trust: A staker always has the option to self-delegate and operate the nodes for AVSs or delegate it to a trusted operator. In this scenario, the staker trusts the operator to perform only the stipulated operations and not engage in any malicious activities. This practice is common in the real world, where service providers like AWS offer services.