Despite recent controversies surrounding its airdrop, there is no doubt that EigenLayer has emerged as one of the most prominent projects of 2024, thanks to its Re-staking mechanism. This mechanism has not only driven a surge in TVL but also prompted users to move their funds and confidence back to the Ethereum ecosystem, away from the frenzy of meme coins.

According to public data, as of the time of writing, EigenLayer's ETH TVL has surpassed 5 million ETH, and the staking amount of its token, Eigen, has exceeded 54 million tokens. The number of active AVS (Actively Validated Services) and Operators stands at 11 and 251, respectively. The EigenLayer ecosystem is also booming, with over 20 leading projects across various sectors, including Lumoz, Espresso, Near, and Dodo, actively participating.

This marks the beginning of a revolution aimed at reshaping blockchain security and profitability around ETH, leveraging EigenLayer. This article will use Lumoz as a case study to delve into the series of technical explorations conducted on EigenLayer, thereby further advancing the technology of Ethereum and the broader blockchain industry.

# 1. Lumoz Launches AVS Computation Layer Based on EigenLayer

As a leader in modular computing layers and ZKRaas Platform, Lumoz has not only performed exceptionally well in the capital markets but has also continuously innovated in the technical field. In April 2024, Lumoz first announced the completion of its Pre-A financing round (with a current valuation of up to $300 million), and shortly thereafter, it announced support for Op Stack + ZK Fraud Proof Layer 2 architecture, pioneering a new model for L2 architecture.

This week, Lumoz officially announced the launch of an AVS computation layer based on EigenLayer, composed of zkProver and zkVerifier, which significantly enhances computational power and security.

Lumoz's zkProver focuses on generating Zero-Knowledge Proofs (ZKP), verifying the authenticity of data without revealing the specific data itself. With powerful computational resources, zkProver can quickly generate efficient Zero-Knowledge Proofs, significantly improving the privacy and security of blockchain networks. zkVerifier, on the other hand, is responsible for verifying these Zero-Knowledge Proofs, ensuring their correctness and reliability. Combined with EigenLayer's Re-staking mechanism, zkVerifier not only leverages Ethereum's security but also provides additional economic incentives for validators. This dual verification mechanism greatly enhances the overall security of the network and reduces trust risks.

Note: EigenLayer's Re-staking mechanism enhances the security of the Ethereum ecosystem by providing AVS, addressing trust issues and the burden of capital costs.

By integrating powerful computational resources with EigenLayer's Re-staking mechanism, Lumoz has created an efficient and secure computational service ecosystem. This innovation not only improves the computational power and security of blockchain networks but also provides developers and users with more application scenarios and value. Through zkProver and zkVerifier, Lumoz brings unprecedented innovation and value to the blockchain field, driving technological advancement across the entire industry.

# 2. Lumoz Computation Layer

The Lumoz Computation Layer architecture is a highly integrated and collaborative system, with its main components and functionalities as follows:

[

1920×1944 256 KB

](https://ethresear.ch/uploads/default/original/3X/4/f/4fa2829a63a584f7eb2b536f543482ae1f2286ee.jpeg)

The main components include:

- Ethereum

: Utilizes the EigenLayer standard to build Active Verification Services (AVS). The staking mechanism of EigenLayer enhances the security of AVS.

- EVM Chain

: Supports a diverse blockchain environment compatible with the Ethereum Virtual Machine (EVM), including but not limited to Polygon zkEVM, Polygon CDK, ZKStack, and Scroll, ensuring broad compatibility and scalability.

- Lumoz AVS Oracle

: Responsible for acquiring and storing data from EVM-compatible chains, ensuring high availability and integrity of the data, thus providing a solid data foundation for the computation layer.

- Lumoz Chain

: Acts as the core management layer of the entire computation layer, responsible for task scheduling, reward distribution, and the management of zkProver and zkVerifier, including but not limited to the processes of node joining and exiting.

- zkProver

: Nodes that execute specific computational tasks.

- zkVerifier

: Verification nodes that validate the execution results.

Through the close collaboration of these modules, the Lumoz Computation Layer not only provides a secure and efficient computational environment but also, through its modular design, lays a solid foundation for future expansion and upgrades.

# 3. What Problems Can It Solve?

## 3.1 Large-Scale Computational Power Demand

Lumoz provides robust cloud infrastructure support for zero-knowledge proof (ZKP) computations. This support is crucial for ZK-Rollups, a blockchain scaling solution that executes transactions off-chain and uses ZKPs to verify the validity of these transactions. The proofs are then submitted on-chain, reducing the load on the main chain and increasing transaction throughput.

Lumoz Cloud Infrastructure Capabilities:

- Compatibility

: Lumoz's cloud infrastructure is compatible with various ZK-Rollup solutions such as Polygon CDK, zkSync, StarkNet, and Scroll. This means it can serve these different platforms without each platform needing to establish its own infrastructure.

- ZK-PoW Algorithm

: Lumoz combines miners' computational resources with cloud infrastructure through the Zero-Knowledge Proof of Work (ZK-PoW) algorithm, enabling miners to contribute their computational power to support ZKP computations.

- Performance and Efficiency

: By supporting parallel computation for ZKPs, computational efficiency is significantly improved as multiple tasks can be executed simultaneously. Additionally, sequential submission ensures orderly processing of transactions.

- Recursive Aggregation Algorithm

: Optimizing the recursive aggregation algorithm reduces the number of required ZKPs, thereby lowering computational complexity and costs.

- Network Communication Improvements

: Enhancements in network communication reduce data transmission time, improving the overall system response speed.

- Cost-Effectiveness

: Through the aforementioned optimizations, Lumoz can reduce the costs associated with ZKP computations, making ZK-Rollup solutions more economically efficient.

Lumoz's cloud infrastructure provides a powerful, flexible, and cost-effective solution for ZKP computations, contributing to the advancement and application of blockchain technology.

## 3.2 Reducing zk Proof Gas

The design strategy of zkVerifier aims to enhance efficiency, scalability, and effectively reduce transaction costs, as reflected in the following aspects:

- Integration of Multiple Proof Sources

: zkVerifier can integrate proofs from different sources, supporting a wide range of zero-knowledge proof applications. This flexibility is a key advantage in the blockchain ecosystem, as it allows various projects and applications to utilize zkVerifier services.

- Gas Cost Savings

: Through meticulously designed proof processing and verification mechanisms, zkVerifier significantly reduces the gas cost

of submitting proofs, providing users with a more cost-effective blockchain service experience.

- Adaptability to Proof Characteristics

: zkVerifier demonstrates adaptability to the characteristics of proofs generated by different proof systems, including proof size, verification time, and verification logic. This adaptability is central to ensuring the efficient operation of the system.

- Customized Release Strategies

: Based on the characteristics of different proofs, zkVerifier has designed customized release strategies that optimize the use of on-chain resources and ensure efficient proof transmission, helping to reduce network congestion and improve transaction speed.

- Deployment of Dedicated Verifiers

: zkVerifier deploys dedicated verifiers, which are key mechanisms to ensure proof validity. These verifiers ensure that only verified proofs can be published to Ethereum, maintaining the security and reliability of the system.

- Optimization of Data Availability Layer

: zkVerifier's data availability layer ensures the durability and accessibility of proofs while providing a cost-effective storage strategy, which is crucial for reducing the operational costs of the system.

- Deep Integration with Ethereum

: zkVerifier publishes verification results to Ethereum, where Ethereum generates verification proofs. This step is crucial for ensuring cross-chain interoperability and trust, facilitating seamless collaboration between zkVerifier and major blockchain networks like Ethereum.

- Authority of Verification Proofs

: The verification proofs generated by Ethereum provide the final authoritative confirmation of the data validity provided by zkVerifier. This is essential for establishing trust in zkVerifier data within the Ethereum network.

These innovative designs of zkVerifier not only address the challenges faced by existing blockchain technology but also achieve significant advancements in enhancing efficiency, reducing costs, and improving interoperability. This design helps to promote the broader application of blockchain technology and provides users with a more secure and efficient service environment.

# 4. Detailed Workflow

## 4.1 zkProver

zkProver is the core component responsible for generating zero-knowledge proofs (ZKPs). ZKPs allow the prover to demonstrate the correctness of a certain assertion to the verifier without revealing any additional information. zkProver includes various types of provers such as zkRollup Prover, zkFraud Prover, and zkML Prover, each optimized for specific computational tasks to ensure optimal performance and system efficiency within their respective domains.

[

1548×1098 126 KB

](https://ethresear.ch/uploads/default/original/3X/3/e/3eff1a5965e046e6f0ad163d4be95e74257d330c.jpeg)

Workflow:

1. Task Acquisition:

The Lumoz AVS Oracle and Dispatch module retrieve tasks from the blockchain and synchronize them to the Lumoz Chain. These tasks consist of assertions or computations that require proof.

1. Task Distribution:

Tasks are distributed to different Provers via the Dispatch module. Acting as the task scheduling center, Dispatch determines which type of Prover is best suited to handle each task based on its nature and requirements. The Dispatch module dynamically allocates computational resources through intelligent algorithms, optimizing resource distribution in real-time based on task load and the performance of each Prover, ensuring stable system operation during high-demand periods.

1. **Proof Generation:**a, zkRollup Prover:

Focuses on generating proofs related to transaction batch compression, enhancing blockchain processing speed and scalability.b, zkFraud Prover:

Generates fraud proofs that help detect and prevent improper behavior.c, zkML Prover:

Specializes in generating complex proofs related to machine learning model verification, ensuring the validity of model outputs without revealing the model itself or its input data.d, Other Provers:

Handle specific types of proofs as needed.

1. Proof Submission:

The generated proofs are sent to the Lumoz Chain for verification and archiving.

### 4.2 zkVerifier

zkVerifier is another key component in the architecture, responsible for verifying the ZKPs generated by zkProver. It ensures the correctness and validity of the proofs submitted to the chain, thereby safeguarding the trust and security of the system. Through an optimized verification process, zkVerifier efficiently handles proofs, reducing operational costs and gas consumption.

[

1548×1373 154 KB

](https://ethresear.ch/uploads/default/original/3X/6/4/64136a1901b29ae5be439c939975916683752c1d.jpeg)

Workflow:

1. Proof Submission: Proofs generated by zkProver are submitted to the Lumoz Chain, initiating the verification task.
2. Proof Verification: The Lumoz Chain sends the verification task to multiple zkVerifiers, which independently perform distributed verification.
3. Collective Decision: At least two-thirds of the verification nodes confirm the proof’s validity, ensuring the authority and consistency of the verification results.
4. Verification Result Processing: Valid proofs and their results are transmitted back to the Lumoz Proof Contract on the blockchain by the Lumoz AVS Oracle. The Task Manager Contract records and responds to the task results on the Lumoz Chain.

## Summary

Lumoz announces the launch of zkProver and zkVerifier based on EigenLayer, significantly enhancing the efficiency of computation and verification. The re-staking mechanism of EigenLayer effectively ensures the security and profitability of the entire service process. With specialized node design, Lumoz can provide solutions for different computational tasks, achieving optimal performance and efficiency. Additionally, through the re-staking mechanism, Lumoz offers substantial returns to stakers, further enhancing the economic security of the system.

In the future, we hope to see more projects like EigenLayer and Lumoz emerge, addressing current blockchain challenges, genuinely solving user pain points, and actively exploring and attempting more efficient and secure solutions. This will ultimately drive the progress and prosperity of the entire industry.