

FortLayer: The Restaking-Powered Risk-Pooling Network on Solana

team@fortlayer.com

V1.0, June 2024

Abstract

This paper introduces FortLayer, a risk pooling network leveraging restaking mechanism on Solana for shared security. By combining Web3 restaking practices with traditional risk pooling techniques, FortLayer aims to secure the decentralized applications on Solana. Risk pooling has similar properties to restaking, both involving collective risk sharing and economic incentives. FortLayer leverages these overlapping principles to build up a safety net for all of the Solana ecosystem.

1 Restaking on Ethereum

Restaking in the Ethereum ecosystem has achieved a critical mass, spearheaded by EigenLayer [1]. This approach allows participants to reuse their liquid staking derivative (LSD) assets to enhancing the crypto-economic security and stability of blockchain infrastructures, referred as Active Validated Services (AVS). Restaking enables assets already staked in Ethereum's Proof-of-Stake (PoS) network to be re-staked in multiple ecosystem protocols, generating new liquid restaking tokens (LRT). This process creates new economic incentives and strengthens security and participation across Ethereum.

Currently, over 32 million ETH (\$120 billion), is staked in Ethereum's PoS network. Of this, around \$20 billion in staked ETH has been restaked into EigenLayer and its ecosystem, representing over 16% of all staked ETH. These figures highlight the significant adoption and trust restaking has achieved within the community.

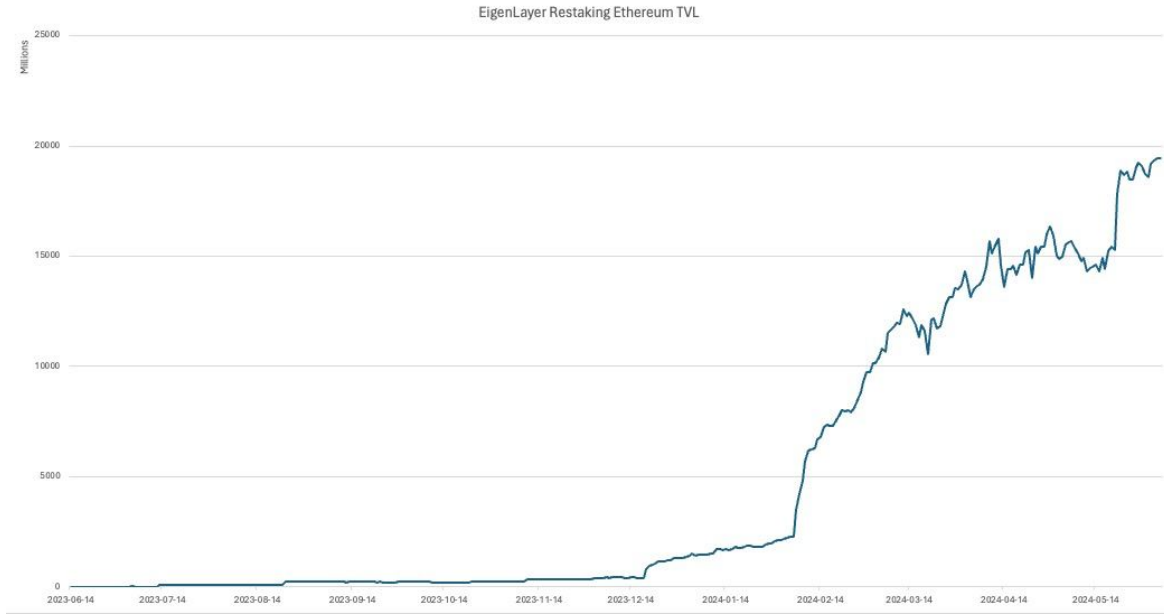


Figure 1: EigenLayer Restaking Growth

While we applaud EigenLayer’s innovation and celebrate its remarkable success, it is important to recognise that there is still much to be done. Despite the substantial restaked assets, the adoption of providing security to AVS (Active Validated Service) remains limited. The true success of restaking should not be measured solely by the volume of restaked assets but also by the breadth and depth of its applications. More use cases are needed, and the operational model, especially the slashing and compensation mechanism, requires further clarity and real-world testing.

2 Challenges of Restaking on Solana

Given the success of restaking on Ethereum, a natural question arises: is it possible to build similar restaking models on other blockchain ecosystems, specifically Solana? Despite Solana’s robust Proof of History (PoH) mechanism and thriving ecosystem, staking - let alone restaking - has not gained significant traction. Our research indicates several reasons for this discrepancy [2] [3]:

2.1 Distinct Consensus Algorithm

Ethereum’s transition to PoS has integrated staking into its security model, where validators lock their ETH to secure the network and earn rewards. In contrast, Solana employs a unique combination of Proof of History (PoH) and PoS. PoH provides a verifiable sequence of events, ensuring a historical record of transactions, while PoS

validates and secures these transactions. This dual approach prioritizes high throughput and low latency, complicating the implementation of a similar restaking model.

2.2 Contrasting Technical Stack

Ethereum uses a modular technology stack that includes infrastructure components like Roll-ups and Data Availability (DA) layers for scalability. Solana, on the other hand, is a monolithic blockchain designed to offer unparalleled performance and throughput. Solana's architecture inherently manages infrastructure concerns, allowing developers to focus on building applications without worrying about underlying infrastructure complexities.

2.3 Different Focus Areas

The focus areas of Ethereum and Solana further highlight their differences. Solana has prioritized high-performance applications such as DePIN, AI, DeFi, and GameFi, where usability and performance is critical.

Restaking, however, focuses on the crypto-economic security of infrastructure components, which does not directly align with the specific needs of these end-user oriented applications. As a result, the demand and use cases for restaking solutions on Solana has been limited.

Given these factors, integrating EigenLayer directly into Solana does not seem feasible. While a similar restaking protocol on Solana for crypto-economic security is possible, its demand and necessity remains questionable.

On the other hand, our engagement with the wider Solana builder communities has revealed a significant demand for risk management solutions. There is an urgent and strong need for coverage against cyber, operational, financial and other risks that the builders and users have been facing, which is currently in substantial shortage of supply. Addressing this pressing need is paramount.

This leads to a pivotal question: Can we leverage the restaking flywheel to meet the specific security demand of the Solana ecosystem?

3 The FortLayer Thesis

In light of the discussions above, FortLayer proposes a novel approach that leverages restaked assets to bolster security through a risk-pooling model. This methodology

does not only address the crypto-economic security as other restaking protocols have been advocating, but also extends practical coverage to a broader spectrum of risks, including cyber, operational and financial risks for various decentralized applications within the Solana ecosystem.

Effectively, FortLayer aims to establish itself as the premier economic resilience and risk covering protocol on Solana by implementing this mechanism. This will enable developers within the Solana ecosystem to fully capitalize on Solana’s high performance and scalability, all while benefiting from an enhanced safety net.

Besides the benefits for the ecosystem, we see several other catalysts for staking of LSDs on Solana. Chief of all, Solana’s current emission rates create significant supply inflation – a challenge that LRTs can effectively mitigate. By staking LSDs into FortLayer, participants can integrate more seamlessly with the entire Solana ecosystem, rather than allowing their assets to remain idle.

4 Understanding Risk Pooling

Before diving deeper into our proposed approach, it is essential to understand the concept of risk pooling. Risk pooling is a well-established practice in the finance industry, where participants collectively share and manage risk with an economic incentive structure. By pooling resources, participants protect themselves or counterparties against significant risks that would be unmanageable individually. This collective approach distributes the financial burden across many participants, enhancing the capacity to absorb losses, providing a safety net, and reducing overall risk [5] [6] [7] [8].

One of the key benefits of risk pooling is promoting stability and predictability in uncertain events, a necessary protective tool across all blockchains. Therefore, an effective risk pooling method will require prudent risk assessments and risk distribution—areas where current restaking primitives fall short.



Figure 2: Risk Pool Model

Typical practices of risk pooling include Industry Loss Warranties (ILW), Risk Sharing Groups, Disaster Risk Reduction, Captives, Mutual, and General (Re)Insurance among others. These methods have been effective and widely adopted across various industries, showcasing their longstanding benefit.

5 Risk Pooling and Restaking Commonalities

While risk pooling and restaking come from different contexts and serve different purposes, they share common principles of collective risk management and economic incentives.

5.1 Differences

- **Risk Pooling:** Focuses on financial risk coverage, pooling resources to cover potential losses for specific, well-defined risks, and promote stability and predictability of risk events.
- **Restaking:** Focuses on crypto-economic risks, leveraging a common security framework to protect multiple blockchain infrastructure components. However, the risks to be covered are yet to be defined with more clarity.

5.2 Commonality

Both models involve a collective approach to risk management and rely on economic incentives to encourage participation. This similarity provides a critical perspective for creating an innovation that combines both models, leveraging their strengths to enhance security and economic stability in blockchain ecosystems.

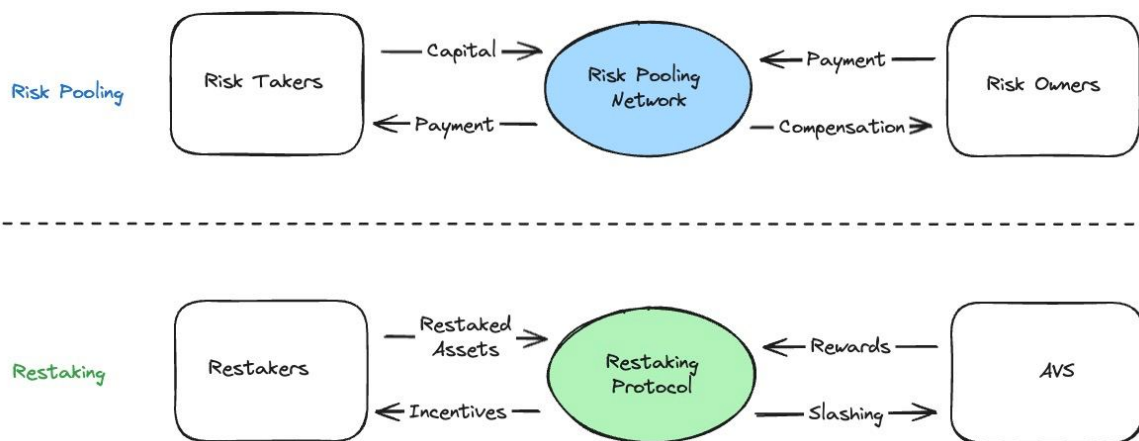


Figure 3: Risk Pooling vs Restaking

6 Proposing Our Solution

FortLayer aims to create a novel solution that leverages both restaking and risk pooling mechanisms to enhance security for the Solana ecosystem. Our solution combines asset restaking with risk management techniques used in risk pooling to secure real use cases. This approach addresses not only crypto-economic risks in infrastructure components but also financial and operational risks in decentralized applications such as DePIN, AI, DeFi and GameFi among others, collectively referred to as Actively Protected Services (**APS**).

By restaking assets, participants contribute to an asset pool for economic incentives. Through risk pooling, these restaked assets are utilized to underwrite specific risks in a prudent manner. Unlike the EigenLayer model, FortLayer places a supplementary focus on risk protection for APS. We incorporate risk management expertise such as risk profiling, analysis, underwriting, and compensation models, to enhance security.

APS will pay for this security service and receive proper compensation in case of event triggers. These security services will be offered via a user-friendly front end, as well as API/SDK integrations for seamless application integration.

Overall, our solution is more application-centric, with an adoption-driven mindset to build for real security use cases.

7 Solution Design

Both restaking and risk pooling involve two main components: assets and risks. Assets are pooled together via restaking and used for risk coverage to gain economic incentives. There will be four main components across the FortLayer network:

1. **Restaking Layer:** Participants restake their liquid assets, forming the basis of the underwriting pool and gaining economic incentives.
2. **Underwriting Layer:** Focuses on risk profiling and pricing, capacity allocations, and policy lifecycle management.
3. **Attestation Layer:** Verifies and attests to the integrity and security of covered parties, making decisions on slashing and compensation.
4. **Economic Layer:** Manages incentives and compensation, ensuring stakeholders in the network are rewarded for their contributions and that covered parties are properly compensated.

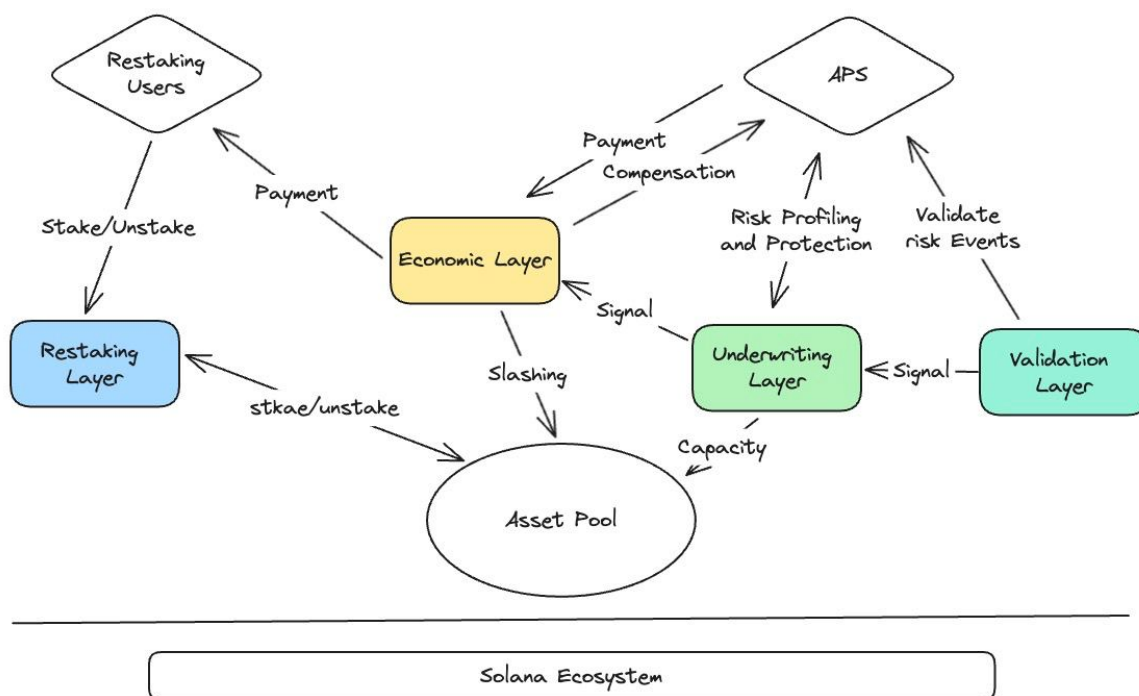


Figure 4: FortLayer Solution Architecture

FortLayer will also accept not only SOL and its liquid tokens but also other assets, particularly bridged BTC, to build its asset pool and enhance security. Asset stakers will receive economic incentives including fees and rewards from the APS.

8 Roadmap

FortLayer Network will be built and launched in 4 phases progressively in the coming months, including:

Phase 1: Dawn

- Initiate development and community engagement.
- Launch initial restaking pools.

Phase 2: Ascend

- Expand asset support and incentive mechanisms (no PointFi).
- Launch the underwriting layer.

Phase 3: Zenith

- Launch the attestation layer and network in full function.
- Expand network functionality and adoption.

Phase 4: Panorama

- Optimize and scale the network.
- Broaden ecosystem partnerships.

9 About the Team

FortLayer Network is built by MetaRisk Labs, the Web3 development firm for Amulet Protocol, the first and only DeFi insurance platform on Solana since 2022. The team has extensive experience in building and operating risk management solutions in the digital asset space. With a proven track record in Web3 risk management and deep roots in the Solana Ecosystem, our team is poised to provide a strong foundation for developing robust Web3 solutions to secure growing decentralized ecosystems.

10 Conclusion

FortLayer aims to pioneer a new approach to restaking on Solana by focusing on application-centric risk pooling. By leveraging our expertise in risk management and the unique capabilities of the Solana blockchain, we are poised to enhance the security and reliability of decentralized applications across the ecosystem.

References

- [1] EigenLayer Whitepaper. <https://docs.eigenlayer.xyz/eigenlayer/overview/whitepaper>
- [2] EigenLayer TVL Growth. <https://defillama.com/protocol/eigenlayer#information>
- [3] Solana Whitepaper. <https://solana.com/solana-whitepaper.pdf>
- [4] Ethereum Scaling. <https://ethereum.org/en/developers/docs/scaling/>
- [5] Risk Pooling. https://www.researchgate.net/publication/226870408_Risk_Pooling
- [6] Risk Pooling, A Technique to manage Risk in Supply Chain Management. https://www.researchgate.net/publication/311451259_Risk_Pooling_A_Technique_to_manage_Risk_in_Supply_Chain_Management
- [7] Design Principles for Risk Pooling. <https://www.nature.com/articles/s41562-021-01121-9>
- [8] Centralization versus Decentralisation: Risk Pooling, Risk Diversification, and Supply Chain Disruptions. https://engineering.lehigh.edu/sites/engineering.lehigh.edu/files/_DEPARTMENTS/ise/pdf/tech-papers/11/11w_002.pdf