Stateless Litepaper

Joseph Habel Jessica Daugherty

1 Introduction

Stateless is a risk management protocol and analytics platform designed to mitigate the vulnerabilities associated with offchain data interactions and computation in blockchain, AI, and DeCompute networks. By enabling secure, reliable, and transparent data flows between decentralized applications (dApps), networks, and data providers with a framework for data verification, risk analysis, and settlement, Stateless addresses critical vulnerabilities in decentralized networks with minimal changes to existing codebases.

2 Problem Statement

Decentralized applications (dApps) rely extensively on third-party data and offchain computations, but these interactions lack robust verification standards and log-level traceability. This absence leaves stakeholders, including users and developers, vulnerable to various risks, such as data manipulation, service degradation, and financial loss, with no reliable way to verify or measure the integrity of the data they consume.

Current execution design patterns, like those in the Ethereum Execution API and similar decentralized data interfaces, expose critical vulnerabilities when the trust between data consumers (applications) and data providers (RPC nodes, indexers, GPUs/AI models, etc.) is compromised. In these cases, malicious behavior, self-dealing, and poor-quality service are challenging to mitigate in real time and nearly impossible to detect and quantify through retrospective audits. While cryptographic solutions like light clients provide long-term methods for data verification, they are not feasible for immediate implementation across decentralized networks.

Traditional approaches to data verification—whether hardware-based, like embedding public/private key pairs or using trusted execution environments (TEEs), or software-based, such as consensus mechanisms and validity proofs—are often impractical or insufficient. Hardware methods can impose permissioning constraints and require specialized equipment vulnerable to hacks, while software solutions can be too resource-intensive for real-time operations.

2.1 Risks to Applications and Consumers

The risks that certain applications and their consumers face if provider trust is compromised, includes:

- **Indirect Theft of Funds** through maliciously created MEV arbitrage opportunities
- **Direct Theft of Funds** for a significant majority of existing DeFi applications.
- **Exposure to XSS and Malware Distribution** for applications resolving media and code either stored or linked to on chain.

There is current exposure to such attacks in all of the major pillars of the web3 ecosystem including, but not limited to:

- DeFi
- Decentralized Namespaces

- NFTs
- Reusable Account Abstraction Entrypoints (ERC-4337)

3 Solution: Verification Layers, Risk Analysis, and Settlement Protocol

Stateless provides a comprehensive solution for securing decentralized data operations by leveraging our open-source verification standards and advanced risk management framework. Our foundational proof of concept focused on building a frictionless experience for application developers with Verifiable RPC APIs, setting the groundwork for a broader, more robust ecosystem.

Building on this foundation, we have developed a light client framework and a compatibility layer for EVM, both of which are already available. The light client framework enables proof-based verification directly on client devices, enabling decentralized applications (dApps) to verify data integrity without relying on centralized infrastructure. This framework provides cryptographic assurances for every data interaction, ensuring data is secure, auditable, and deterministic.

The EVM compatibility layer enables seamless integration with Ethereum-based environments, allowing developers to adopt our verification standards without significant changes to their existing workflows. By supporting backward compatibility, this layer ensures that any EVM-compatible network can utilize our verification tools, expanding the reach and utility of our standards across multiple decentralized platforms.

3.1 Application Proxy and Data Collection

Applications can utilize our proxy service to route their data through Stateless, enabling real-time verification and analysis without needing their networks or providers to change their existing setups. This flexibility ensures that the application can still benefit from Stateless's security and risk management services even if a provider has not yet adopted our verification standard. The proxy layer acts as an intermediary, normalizing data into a format our analytics platform can process.

By collecting this request/response data, Stateless builds a robust data lake that supports public and private insights. This data informs our risk models, contributing to a dynamic risk prediction market that adjusts coverage requirements and drives automated settlements based on real-time assessments.

3.2 Data Analytics, Prediction, and Risk Management

The stateless platform offers advanced analytics capabilities that turn raw data into actionable insights. Our analytics engine continuously evaluates risk based on aggregated data from diverse decentralized compute environments, including those using non-standard infrastructure. This data allows organizations to see how users interact with their frontends, detect bots, and identify issues such as incorrect pricing or misdirected tokens.

These insights support a dynamic risk prediction market, allowing for real-time adjustments to risk levels and enhancing the ecosystem's overall security. By providing a comprehensive understanding of risk exposure, the Stateless platform enables networks, applications, and organizations to proactively address vulnerabilities, ensuring a secure and resilient environment for decentralized operations.

3.2.1 Tokenomics and Protocol Actors

The Stateless Protocol utilizes the SSL token to underpin its economic model, ensuring secure and reliable interactions within its ecosystem. The tokenomics strategy aims to balance long-term protocol health with the needs of users, providers, and other participants. Below is an overview of the key design decisions, token dynamics, and initial use cases.

Pool Managers: Pool Managers ("Managers") develop pool strategies and manage those strategies. For their role, Managers earn a percentage of the fees created by the pool, dictated by the Pool Manager. A reader may liken these to providers on EigenLayer where restakers are relying on the provider to provide security/services to AVSs but are punished if the provider fails to provide good services.

Data Providers: Compute Providers ("Providers") run the Stateless client, stake SSL, and provide data to Data Consumers. Responsible for responding to challenge transactions, and validating or invalidating challenges involving third-party providers.

Data Consumers: Data Consumers ("Consumers") consume data and pay into risk pools.

A note: We envision that it may take some time for Stateless to provide frictionless payment mechanisms. We imagine that other parties may pay into the pools in place of the actual data consumer. This approach has its own merits.

Stakers/Restakers: Stakers/Restakers ("Stakers") provide stakes (capital) that protect Consumers and receive payments from Consumers (or other interested parties) in exchange for their risk. Stakers provide governance oversight (by staking SSL) to Managers and arbitration proceedings.

Stakeholders: SSL Stakers ("Stakeholders") acquire and stake SSL on behalf of Managers in one or more pools in exchange for a portion of the management fees of the pools. As management fees increase, so does the real yield for SSL stakeholders. Stakeholders, like Stakers, are keen to profit from participation in the protocol, but might not be willing to accept the risk of participating in a pool. To generate interest and attraction from these individuals, we designed a staking-style mechanism where investors can stake to be eligible for protocol fees in proportion to the amount the investor staked.

4 Roadmap and Future Developments

Stateless is evolving rapidly to address the needs of decentralized applications and infrastructure providers through a comprehensive suite of products, open-source tooling, and a decentralized risk management protocol.

2024 Testnet: The deployment will include the first versions of our public and private risk dashboards, which provide general risk insights and application-specific analytics. These dashboards allow stakeholders to understand potential vulnerabilities and implement data-driven risk mitigation strategies.

At the same time, our existing proof-based consumer light client framework and EVM compatibility layer will be integrated into the testnet. These tools enable seamless interoperability with EVM-compatible networks and decentralized data sources, allowing for direct data verification at the client level and enhancing the security of decentralized applications without relying on centralized infrastructure.

The initial rollout will feature our Proxy and Audit Services, which empower applications to route their data through Stateless for real-time verification and analysis, offering enhanced security with minimal changes to existing network infrastructure.

2025 Mainnet: introduce further enhancements, including advanced risk modeling tools and establishing managed risk pools. These innovations will enable dynamic assessment and management of risk exposure across decentralized networks, providing a robust framework for mitigating potential threats and compensating for any faults detected. We will also launch new capabilities for detecting Sybil attacks and bot activity, expanding the use cases for our risk analysis.

Deploying our comprehensive Data Lake and Analytics Platform, which aggregates data from various decentralized compute environments, will support these enhancements. This platform will provide deep insights into data flows, user interactions, and network performance, supporting risk analysis and prediction models that enable an arbitration and settlement system.

With the data management processes in place, introducing the SSL token will facilitate data-sharing incentives, enable governance participation, and support staking mechanisms for risk coverage, reinforcing the security and reliability of interactions within the ecosystem.

Simultaneously, we will launch specialized AI Execution Risk Dashboards to extend our blockchain risk management framework into the domain of AI model execution. These tools will provide detailed insights into AI models' operational integrity and performance across decentralized environments, ensuring their reliability and security. Finally, we will integrate automated settlement processes with our dynamic prediction market, allowing real-time repricing based on observed risk levels and seamless compensation for verified faults. This integration will create a self-sustaining ecosystem that continuously adapts to maintain trust and security.

5 Conclusion

As decentralized networks become more integral to digital infrastructure, ensuring the integrity and security of offchain data interactions is critical. Stateless is at the forefront of this effort, offering a robust framework for verifying, analyzing, and managing the risks associated with decentralized data. By providing a seamless integration path through open-source tools and advanced analytics, we empower developers and networks to build more secure, reliable applications. Our focus on adaptability and comprehensive risk management prepares the ecosystem to address emerging challenges and confidently drive forward. Stateless is not just enhancing data security—it's laying the groundwork for a more trustworthy and resilient decentralized future.