Stateless Litepaper

Joseph Habel Jessica Daugherty

1 Introduction

Stateless is a verifiability protocol focused on addressing the middleware needs of decentralized networks. This initiative was born out of the recognition that various attack vectors exist within the design patterns of existing web3 applications, with significant exposure in the Ethereum ecosystem. Stateless aims to mitigate these risks by providing a robust middleware solution, allowing application developers to provide their users with enhanced security when interacting with distributed systems.

2 Problem Statement

The design patterns encouraged by the current Ethereum Execution API and other blockchain APIs which have taken inspiration from Ethereum have attack vectors that exist in situations of compromised operational trust between an application interface acting as an RPC consumer and an independent RPC provider. Should that operational trust be compromised, these attacks **cannot currently be mitigated** in real-time and **cannot be detected historically** in an audit of event logs. Proposed solutions such as light clients provide long-term, cryptographic approaches to address these issues. However, they are not near-term applicable, leaving applications and users currently exposed to risks.

2.1 Risks to Applications

The risks that certain applications 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)

2.2 Limitations of Current Infrastructure Providers

Existing solutions in the market have some notable limitations, including security, fault tolerance, and decentralization concerns. Centralized infrastructure providers such as Infura and Alchemy have a single point of failure, potentially compromising the security and reliability of applications.

Decentralized providers such as Pocket Network and Lava have even lower barriers to entry, requiring a nominal financial investment to begin serving data to production applications. These network protocols

lack any direct protection for application developers, and can inadvertently reward bad actors who serve fraudulent and malicious data.

3 Stateless Middleware: A Solution

Stateless is designed to address the security needs of blockchain application developers and their users by providing a middleware solution that enhances security without the need for developers to make any changes to their existing codebase. Stateless middleware allows applications to utilize multiple independent provider sources, requiring a malicious actor to compromise multiple independent providers simultaneously, as opposed to the current landscape which only requires one.

3.1 Enhanced Security for All

Stateless middleware enables applications to add a mitigation layer simply by wrapping their API provider layer, minimizing any changes to just at most a few lines of code. Given the open development nature of blockchain applications, and the prevalence of forks across the ecosystem, it was essential to allow any developer to easily protect their users, regardless if they sufficiently understood the original code to adapt it in response to the public disclosure of the existing attack vectors.

While the issues identified have the most pronounced impact in the Ethereum ecosystem, Stateless middleware is designed to be adaptable to various blockchain and decentralized networks, ensuring that the provided security enhancements can be applied to a wider range of decentralized application development.

3.2 Stateless From the Perspective of an Application Developer

The first iteration of Stateless will be focused on building a frictionless experience for application developers to secure their existing applications.

Application developers will have access to both a CLI and HTTPS API for managing "buckets" of independent providers. The application will be able to select as many providers as they wish to attempt to source data from, as well as the number of attestations they require to accept that data, similar to the experience of setting up a multisig Safe wallet. Developers will have full control of any performance trade-offs that would be made from now sourcing data from multiple providers, and will have a clear picture of the impacts of their choices. Developers will be able to modify and view their existing buckets either interactively through the CLI, or programmatically in their existing CI/CD pipelines.

Once their bucket has been setup, developers will be able to create an invoice contract to manage the billing of any buckets that they've created. Once that invoice contract has been deployed, anyone is able to send a custom restricted ERC-20 token functioning as Compute Credits to that invoice contract. The Compute Credit ERC-20 will not be a liquid speculative token. This token will only be exchangeable for whitelisted stablecoins, and can only be sent to existing invoices or returned back for stablecoins. Once the credits have been sent to the invoice, any usage will be drawn out of that invoice by an account owned by Stateless based on observed network usage. The invoice owner will be free to stop billing and withdraw any remaining credits at any point in time.

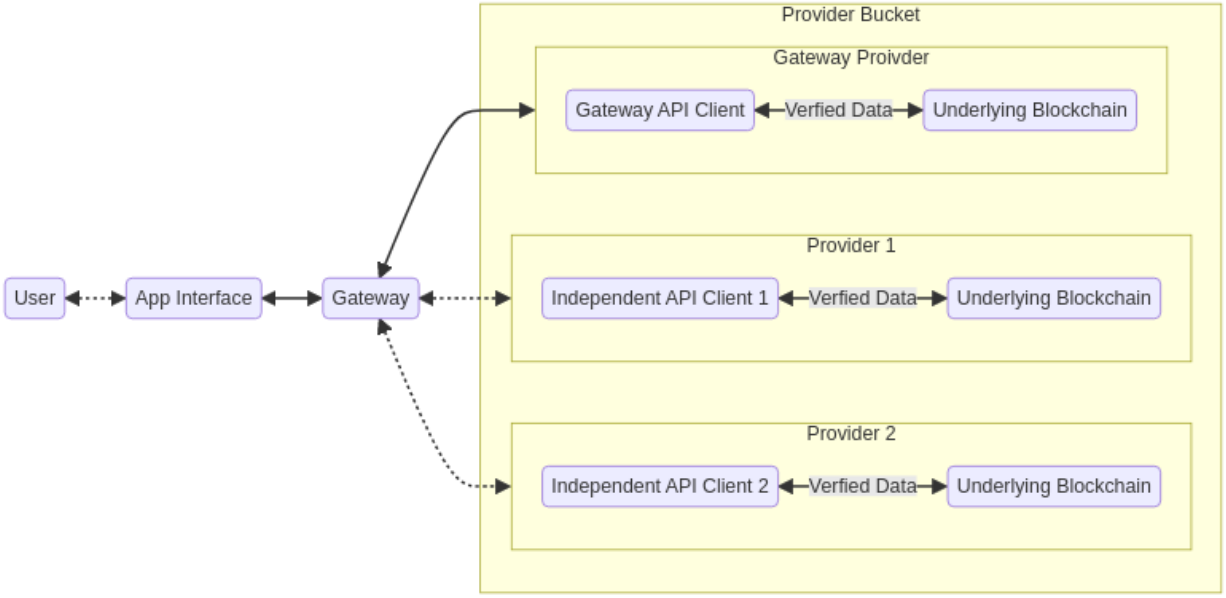
Finally, the experience of integrating the provider bucket can be as simple as replacing the existing RPC URL in the interface if the developer chooses, or to eliminate any integrity trust, simply wrapping their existing provider with a lightweight wrapper. Minimizing any code changes in their existing codebase to as little as possible.

4 Roadmap and Future Developments

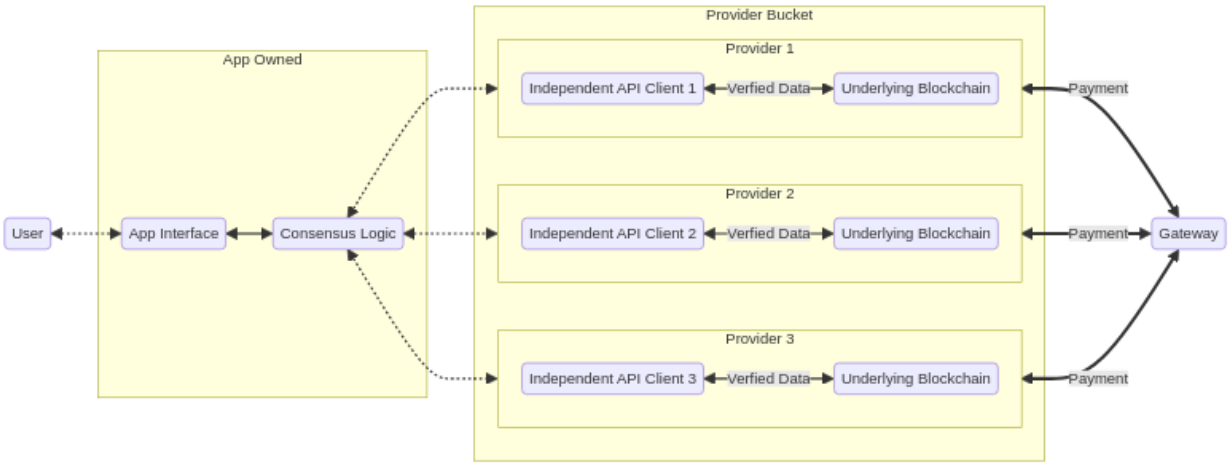
Stateless has a clear roadmap for its development, focusing on both short-term and long-term goals that aim to introduce critical decentralized infrastructure while remaining in step with the evolutions of current and upcoming data networks.

Stateless aims to redefine the middleware landscape space by offering a secure and auditable API middleware solution that mitigates vulnerabilities between consumer requests and data node responses. The goal is to protect end consumers from data integrity failures and financial exploitation, ensuring a secure and efficient interface for both user access points and providers.

2023: Launch permissioned decentralized middleware. This milestone focuses on developing and deploying a secure and fault-tolerant middleware solution that addresses the limitations of current offerings and provides applications with client side request verification.



2024-2025: Enhancing the autonomy of our users by expanding the range of tools available to data consumers, with a focus on integrating Infrastructure as Code (IaC) workflows, comprehensive integrated environments, and extensive tracing capabilities. These enhancements aim to increase application resilience and reduce dependency on the Stateless gateway, thereby mitigating potential points of failure and ensuring continuity of service.

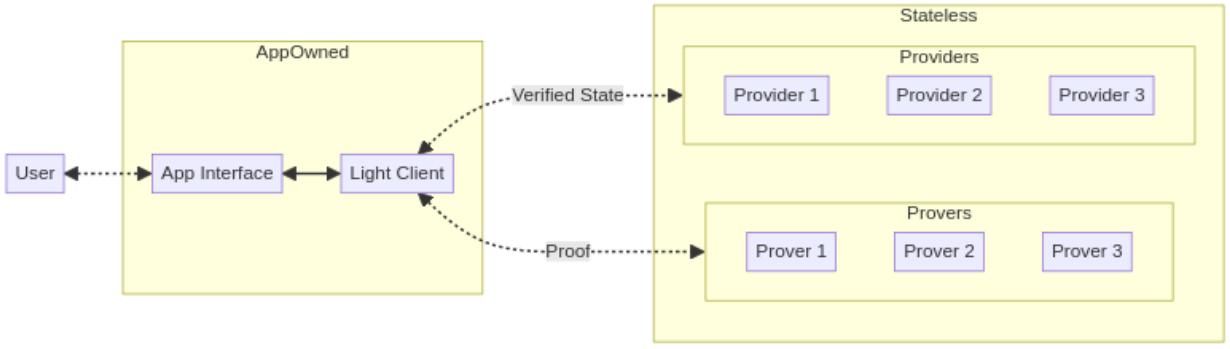


Leveraging our legacy verification services, Stateless will begin introducing proof services, a consumable light client, and extend safety guarantees to encompass indexing and streaming analytics, enhanced by value-add APIs, and support for non-blockchain computations such as peer-to-peer or LLM networks.

Stateless's ZK initiatives aim to solidify the infrastructure that underpins both Layer 1 and Layer 2 solutions (L2s) by providing verifiable state for consumer light clients and proving the sequence of transactions before they are submitted to the base Layer 1 (L1) chain. This vital service aims to revolutionize the credibility and efficiency of the interactions between applications and various blockchain networks.

Through a federated but heterogeneous node network, Stateless encourages data providers to continually refine and enhance their services and provers, fostering a cooperative environment with a diverse range of complementary offerings.This strategic development positions Stateless as a comprehensive "one-stop" infrastructure solution where consumers can not only access verifiable RPC but also choose from a variety of proof-based services tailored to their specific use cases.

2026: Establish a decentralized prover market that enhances the integrity and efficiency of decentralized ecosystems by catalyzing direct peer-to-peer connection, consumption, and payment between consumers and nodes. This permissionless ecosystem, built on the foundation of verifiable compute, ensures the trustworthiness and transparency of every interaction. With blockchain-agnostic proof infrastructure, Stateless enables the client-side validation of data requests across any supported network or service through a combination of trust-minimized and trustless operations.



As the Stateless protocol matures, the existing compute credit system will evolve into a fully-fledged economy, underpinning the marketplace with a token-based model that encapsulates both transactional fluidity and incentivized participation. These compute credits, integral to our operational framework, will transition to facilitate not just transactional exchanges but drive additional economic activities within the network that

bolster the demand side needs of the network.

The token economy is designed to support advanced verification processes and ensure they remain seamless as the network scales. Compensation is tightly linked to service quality through the protocol's native ability to audit work performed and measure performance metrics. This design maintains a close coupling of service excellence with appropriate rewards, promoting a high-performance standard across the network. Network equilibrium is further achieved through stakeholder participation in subsidizing operations, enhancing security, and reinforcing quality, advocating for demand side network effects and preventing operator-centric governance.

This evolution is redefines how decentralized infrastructure is accessed, offering secure, direct, and cost-effective transactions that align with the varied demands of various communities, seeking to eliminate the vulnerabilities associated with intermediary gateways, thus significantly bolstering market efficiency, security, and reliability.

5 Conclusion

In the evolving landscape of decentralized ecosystems, the necessity for secure, efficient, and transparent middleware solutions is undeniable. Stateless emerges in response to this need, targeting critical vulnerabilities in decentralized data execution and offering a seamless solution that redefines the interaction between networks and users.

Our vision extends beyond mitigating risks. We aim to transform the infrastructure of decentralized data interaction, ensuring verifiable computation and integrity become the bedrock of decentralized data operations. Stateless is shaping a future where trust-minimized operations replace trusted gateways, fostering a more secure, efficient, and inclusive digital economy.

In the emerging proof-based paradigm, Stateless is the bridge for closing the gap on this transition toward a model of data autonomy replacing trusted intermediaries with verifiable, transparent, and efficient access points. As we stand at the forefront of this transformative era, Stateless is not just building solutions; we are pioneering a new standard in the decentralized landscape.