# S3N – Serverless TEE Network

Ewanretor Giwa-Okugbe

ZERO Labs

# Abstract

S3N is a serverless computing platform that leverages Trusted Execution Environments (TEEs) to provide a secure, scalable, and verifiable infrastructure for confidential applications. The aim of this paper is to propose a way to efficiently run applications securely, and confidentially on the edge.

By abstracting the complexities of TEE management and enforcing cryptographic attestation, S3N allows developers to focus on business logic while benefiting from hardware-backed security guarantees.

**Disclaimer:** This is an incomplete draft document. We welcome comments, critiques, and improvements. Nothing in this document is a promise or guarantee of any kind.


## 1. Introduction

Deploying applications on TEEs remains a complex challenge. Developers must navigate Trusted Computing Base (TCB) requirements, partition applications into heterogeneous execution models, and contend with limited tooling for seamless deployment. Unlike cloud-native platforms like Cloudflare Workers or Vercel, TEE-based deployments lack a one-click solution for secure execution at scale.

### 1.1 Addressing the issues from first principles

Working with TEEs has evolved significantly since the early days of Intel SGX, largely due to Intel TDX. While SGX confines execution to enclaves, requiring manual workload partitioning and complex enclave calls, TDX runs entire VMs in an encrypted environment, shifting the trust boundary to the VM itself. This eliminates fine-grained enclave management while maintaining confidentiality and integrity against the host and hypervisor.

Working with TDX , our focus shifts to structuring the VM efficiently rather than managing enclaves. For S3N, we introduce Slipstream, a lightweight, high-performance micro-VM designed for confidential compute at the edge. Inspired by the efficiency of Firecracker, and leveraging pre-eminent work such as Dstack-TEE, Slipstream is optimized for rapid startup, low overhead, and secure execution across a distributed network.

**Note:** While this paper primarily addresses Intel TDX, the concepts explored are not exclusive to it. We also consider potential support for other TEEs, such as AMD SEV.

### 1.2 Unstoppable edge compute

The main aim with S3N is to enable confidential edge compute that isn't only performant but also highly resilient, with micro-VMs running in distributed,

decentralized environments to ensure near-100% uptime. To achieve this, we're building an AVS on EigenLayer securing our protocol with the decentralisation of Ethereum through the Othentic stack.

## 2. Architecture

- Micro-VM
- Orchestrator
- CDN
- Middleware

## 3. Economics

## 4. Conclusion

## References

[1] Cuckoo Filter