

SAMUEL T. DAHUNSI

ZK & Blockchain Engineer | Rust • Proof Systems • Protocols • Applied Cryptography
dahunsisamuel1st@gmail.com | [GitHub](#) | [LinkedIn](#) | samueldahunsi.me | Nigeria / Remote

SUMMARY

ZK and blockchain engineer building proof-system components, confidential applications, smart contracts, and verifier-oriented protocol flows. Implemented multilinear polynomials, sum-check, GKR, FFTs, and KZG components in Rust; built systems using Noir, UltraHonk, Soroban, Clarity, Solidity, FHE, and browser-side proving. B.Sc. Mathematics with practical experience translating cryptographic identities into code, tests, on-chain verification, and honest security boundaries.

TECHNICAL SKILLS

Languages: Rust, TypeScript, Solidity, Clarity, Go, Python, JavaScript

Proof Systems: multilinear polynomials, sum-check, GKR, FFTs, KZG, Fiat-Shamir, polynomial commitments, pairings

ZK / Cryptography: Noir, UltraHonk, BN254, BLS12-381, Pedersen commitments, zkSNARKs, FHE, selective disclosure

Blockchain / Protocol: Soroban, Stellar, Stacks, sBTC, EVM, Clarity, smart-contract protocols, transaction monitoring

Backend / Testing: Node.js, PostgreSQL, Docker, REST APIs, property-based testing, Foundry, Hardhat, integration testing

SELECTED ZK & PROTOCOL PROJECTS

- **Rust ZK Cryptography Study** (Rust, sum-check, GKR, KZG) - Implemented finite-field and polynomial building blocks from first principles, including multilinear polynomials, interpolation, FFTs, sum-check, GKR, and a multilinear KZG opening prototype with pairing-based verification.
- **Lucent** (Rust, Soroban, Noir, UltraHonk) - Built confidential payment flows with browser-generated proofs, Pedersen-committed balances, native verification, selective disclosure, and a two-step payout design that respects Soroban transaction-size constraints.
- **StellarCred** (Rust, Noir, UltraHonk, BN254) - Built reusable zero-knowledge credential infrastructure with issuer discovery, browser-side proving, selective disclosure, proof registries, and native on-chain verification on Stellar.
- **Privara** (Clarity, TypeScript, SIP-018, secp256k1) - Designed intent-based Stacks settlement using structured signatures, encrypted instructions, nonce and expiry checks, relay execution, replay protection, and explicit privacy limits.

EXPERIENCE

QuikDB Inc | Remote - Co-Founder & Software Engineer

Dec 2025 - Present

- Built backend systems with Node.js, TypeScript, PostgreSQL, MongoDB, and Docker for a community-powered cloud platform running containerized workloads across distributed compute nodes.
- Worked on deployment orchestration, application lifecycle management, node monitoring, restart reliability, live logs, and operational tooling for developers and node operators.
- Contributed to platform architecture and infrastructure trade-offs; produced developer documentation and reference implementations as a supporting responsibility.

Unboxd | Remote - Full-Stack Developer

Apr 2025 - Nov 2025

- Developed backend services in Go and REST APIs for event, guest, and workflow management, including real-time data synchronization across product features.
- Shipped end-to-end product features across backend and frontend using Go, TypeScript, Remix, and Chakra UI in an iterative product environment.

PROTOCOL SECURITY & RESEARCH

- Performed adversarial reviews across DeFi, bridge, and account-abstraction systems, identifying risks in nonce ordering, escrow cancellation, Merkle validation, unchecked token calls, slippage, and solver or user-operation binding.
- Produced vulnerability write-ups centered on violated invariants, concrete attack paths, system impact, and remediation rather than surface-level code observations.
- Built and tested protocol state machines involving proofs, oracles, disputes, slashing, liquidity, escrow, settlement, replay protection, and selective disclosure.

ADDITIONAL CRYPTOGRAPHY WORK

CipherMarket - confidential prediction markets with encrypted positions and dispute flows; Shade - FHE payments with encrypted balances and escrow; VeilDrop - confidential token distribution with private allocations and vesting.

EARLIER ENGINEERING EXPERIENCE

Oakchain | Lagos - Web3 Frontend Developer

Jan 2024 - Oct 2024

- Built TypeScript/React interfaces integrating wallet authentication, transaction signing, and smart-contract interactions for Web3 developer products.

Web3Bridge | Lagos - Solidity Developer Intern

Aug 2023 - Oct 2024

- Built and tested Solidity applications with Foundry/Hardhat-style workflows, wallet integrations, and full-stack decentralized application patterns; developed a foundation in smart-contract security and protocol design.

EDUCATION

Obafemi Awolowo University | Nigeria - B.Sc. Mathematics

2018 - Jul 2023

- Final-year project: numerical methods for option pricing using the Black-Scholes framework, including Ito calculus, PDE formulation, explicit/implicit schemes, and nonlinear-volatility extensions.
- Relevant foundations: linear algebra, real analysis, numerical methods, mathematical modelling, topology, probability/statistical reasoning.

OPEN SOURCE, WRITING & MENTORSHIP

- Maintain a Rust zero-knowledge study repository implementing FFTs, polynomial interpolation, Shamir secret sharing, sum-check, GKR, and KZG components from first principles.
- Published technical writing on multilinear KZG commitments and binding assumptions, connecting quotient identities and pairing checks to concrete Arkworks code.
- Mentored developers in a three-week Web3Bridge ZK program covering commitments, polynomial methods, proof systems, and verifier-oriented reasoning.

[GitHub: zk_cryptography_study](#) | [Portfolio / writing](#)