SAMUEL T. DAHUNSI

Protocol & Software Engineer | Rust • Bitcoin/Stacks • Distributed Systems • Applied Cryptography

dahunsisamuel1st@gmail.com | GitHub | LinkedIn | samueldahunsi.me | Nigeria / Remote

SUMMARY

Protocol-focused software engineer with hands-on experience building Bitcoin-adjacent payment systems, Stacks smart contracts, distributed cloud infrastructure, Rust cryptography prototypes, and security-sensitive blockchain protocols. Built applications using sBTC and STX, implemented protocol logic in Clarity, Rust, Go, Solidity, and TypeScript, and worked across backend services, transaction monitoring, property testing, cryptographic verification, and adversarial protocol analysis. B.Sc. Mathematics with a deliberate focus on Bitcoin, distributed systems, reliability, and applied cryptography.

TECHNICAL SKILLS

Languages: Rust, Go, TypeScript, Solidity, Clarity, Python, JavaScript
Bitcoin / Protocol: Bitcoin, Stacks, sBTC, payment and settlement flows, smart-contract protocols, EVM, Soroban
Backend / Systems: PostgreSQL, MongoDB, Node.js, REST APIs, Docker, Linux, AWS, distributed compute infrastructure
Cryptography / Security: KZG commitments, BLS12-381, pairings, Fiat-Shamir, zkSNARKs, Noir, UltraHonk, FHE, protocol review
Testing / Tooling: Foundry, Hardhat, property-based testing, integration testing, smart-contract testing, benchmarking and debugging

SELECTED PROTOCOL & SYSTEMS PROJECTS

- **StackPay** (Clarity, TypeScript, Stacks, sBTC) - Built Bitcoin-secured payment infrastructure for accepting sBTC and STX through invoices and checkout flows. Implemented Clarity contracts, transaction monitoring, receipts, merchant notifications, webhooks, and property-based tests.
- **Privara** (Clarity, TypeScript, SIP-018) - Built a Stacks payment router using signed intents, encrypted settlement instructions, relayer-submitted transactions, nonce and expiry checks, replay protection, and explicit metadata-reduction boundaries.
- **Rust Multilinear KZG Prototype** (Rust, arkworks, BLS12-381) - Implemented multilinear polynomial commitments and openings with pairing-based verification. Used the prototype to study binding assumptions, elliptic-curve operations, and practical verifier design.
- **Lucent** (Rust, Soroban, Noir, UltraHonk) - Built confidential payments with client-side proofs, committed balances, native verification, selective disclosure, and a two-step payout flow designed around transaction-size constraints.

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.

SECURITY & PROTOCOL ENGINEERING

- Performed adversarial smart-contract and protocol reviews across DeFi, bridge, and account-abstraction systems, identifying issues in nonce ordering, escrow safety, Merkle validation, unchecked token calls, slippage, and 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 oracles, disputes, slashing, liquidity, escrow, settlement, replay protection, and cryptographic verification.

ADDITIONAL PROTOCOL WORK

StellarCred - reusable ZK credentials with browser-side proving and Soroban verification; AgentHub - x402 API settlement on Algorand mainnet; CipherMarket - confidential prediction markets with encrypted positions and dispute flows.

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, translating implementation details into protocol-level reasoning.
- 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