

Binston Cardoza

Independent Engineer

binstoncardoza@gmail.com · +91 9003986431 · Kanyakumari, India · github.com/binsta · linkedin.com/in/binston-sukhael-cardoza

PROFESSIONAL SUMMARY

Independent engineer with 2+ years of professional software engineering and ongoing research in zero-knowledge (ZK) cryptography, Rust systems programming, and EVM smart contract security. Delivered production full-stack applications and REST/GraphQL APIs at Interview Look. Currently building open-source cryptographic infrastructure — ATLAS (ZK circuits, Groth16) and ARGUS (EVM bytecode analysis) — using Rust, Circom, and arkworks. Open to protocol engineering, smart contract security, backend Rust, and distributed systems roles.

TECHNICAL SKILLS

Languages: Rust Go TypeScript JavaScript Python Solidity

ZK & Crypto: Groth16 Circom arkworks zkVM BN254 Grumpkin ZKP Multiset Hashing

Blockchain: EVM bytecode analysis Smart contract security Ethereum Solana/Anchor revm

Web & Backend: Node.js Express.js React.js MongoDB REST APIs GraphQL

Systems & DevOps: Docker Git Linux CI/CD libp2p SSZ Z3 solver

Formal Methods: TLA+ (protocol spec & model checking) Lean4 (cryptographic proof modeling)

PROFESSIONAL EXPERIENCE

Independent Engineer — ATLAS & ARGUS *Remote*

Jul 2023 – Present

- Design and implement Rust-based cryptographic infrastructure for open-source ZK and EVM security research.
- Build algebraic ZK circuits (ATLAS) using Rust, Circom, Groth16, and arkworks; reduced circuit cost to ~30 constraints vs ~7,095 with SHA-256.
- Develop ARGUS: EVM bytecode analysis pipeline — control-flow reconstruction, concolic execution (Z3), and revm fork-state validation. No source or ABI required.
- Apply TLA+ for distributed protocol specification and Lean4 for cryptographic invariant verification.

Software Engineer *Interview Look · Remote*

Jan 2021 – Jun 2023

- Built and maintained production full-stack applications using MongoDB, Express.js, React.js, and Node.js.
- Designed RESTful and GraphQL APIs serving internal dashboards and external client integrations.
- Implemented Docker-based CI/CD pipelines, reducing deployment time and improving release reliability.

OPEN-SOURCE PROJECTS

ATLAS — Algebraic Transform for Low-Constraint Arithmetic Structures

github.com/binsta/atlas

Rust, Circom, Groth16, arkworks · Feb 2026 – Present

- Implements algebraic map-to-curve (ePrint 2025/1503) on Grumpkin/BN254; reduces ZK circuit cost to ~30 constraints vs ~7,095 (SHA-256). Covers zkVM memory consistency and relational BLS for zkPoS.

ARGUS — Automated Runtime Guard for Unverified Smart Contracts

github.com/binsta/argus

Rust, EVM, Z3, revm · Dec 2025 – Present

- Self-contained pipeline: deobfuscation → TAC IR → concolic execution → Z3 synthesis → revm fork-state validation on raw EVM bytecode. No source code or ABI required.

EDUCATION

Bachelor of Technology — Information Technology

Aug 2012 – Jun 2016

Bharath University, Chennai

CERTIFICATIONS & RECOGNITION

- IBM Blockchain Foundation Developer V2 (May 2021 – Present)
- Starknet Community Recognition — snfoundry ecosystem contributor