WASIU AJAO

+2348105309925 | truthixify@gmail.com | LinkedIn | GitHub | Portfolio | **Nigeria**

PROFESSIONAL SUMMARY

Software developer with a hacker mindset, focused on tackling complex problems in low-level systems, cryptography, and decentralized technologies. Passionate about building secure, scalable applications with expertise in Rust, Solidity, and blockchain integrations. Skilled in leveraging cryptographic primitives, zero-knowledge proofs, and smart contract development. Strong background in backend engineering, decentralized systems, and open-source contributions.

CORE SKILLS AND COMPETENCIES

- Programming Languages: Rust, Solidity, Python, JavaScript (ES6/ES7), TypeScript, Go
- Frameworks & Libraries: Anchor, React, ExpressJS, TailwindCSS, Prisma ORM, Fastify
- Development Tools: Docker, Nix, Unix-systems, Git / GitHub / GitLab, Foundry/Hardhat
- Blockchain & Cryptography: Smart Contracts, zk-SNARKs, Ethereum and Solana Development
- Software Development: Backend Engineering, API Design, Microservices, Security, Databases with SQL and NoSQL
- Collaboration & Methodologies: Open-Source Contributions, Technical Documentation

PROFESSIONAL EXPERIENCE

ZK and Smart Contract Intern – Modulo Labs
June 2025 – Present | Remote

- Worked as part of the Panther Protocol support team, assisting users, troubleshooting issues, and ensuring smooth protocol operation.
- Designed, implemented, and tested zero-knowledge circuits in both Noir and Circom, gaining hands-on experience with multiple ZK toolchains.
- Contributed to the Solidity smart contract codebase, implementing features, fixing bugs, and improving maintainability.
- Learned and applied advanced blockchain engineering practices under the mentorship of leading engineers in the ZK and DeFi space.

Open Source Fellow – OnlyDust
April 2025 – Present | Remote

- Promoted to OnlyDust Fellow in recognition of consistent, high-quality contributions across multiple blockchain and Web3 open-source projects.
- Completed quests involving feature implementation, bug fixes, and documentation improvements, directly enhancing project functionality and user experience.
- Collaborated closely with maintainers and core developers to review code, discuss architecture, and refine development practices.
- Strengthened expertise in Git workflows, open-source collaboration, and community-driven development within the blockchain ecosystem.
- Leveraged fellowship opportunities to expand professional networks and engage in high-impact projects across diverse ecosystems.

Open Source Contributor – Privacy, Scaling & Exploration
Dec 2024 – Present | Remote

- Wrote technical documentation and tests to enhance project maintainability.
- Improved user experience on the Good First Issue site by developing a search bar and integrating efficient issue search functionality.

FullStack Intern (TypeScript and Python) – CodeTree
Jan 2025 – April 2025 | Remote

- Contributed to building and customizing internal tools and e-commerce solutions using platforms like Shopify and Retool.
- Used TypeScript and Python to extend no-code platforms, automate workflows, and create reusable components.
- Collaborated closely with cross-functional teams to translate client needs into scalable product features.
- Gained hands-on experience in integrating APIs, managing state, and debugging user-facing applications.

Open Source Contributor – RustCrypto
Dec 2024 – Jan 2025 | Remote

- Implemented the MD6 hash function in Rust, optimizing for performance and security. Developed a Rust implementation of the MD6 cryptographic hash function, ensuring correctness, efficiency, and security compliance. Optimized memory usage and computational performance to meet cryptographic standards.

- Contributed to cryptographic libraries, improving hashing, ciphers, and digital signatures. Enhanced existing RustCrypto libraries by fixing vulnerabilities, improving efficiency, and adding new cryptographic functionalities. Worked on various primitives, including symmetric encryption, hashing algorithms, and digital signature schemes.
- Wrote documentation and tests to ensure correctness and safety in cryptographic primitives. Designed and executed comprehensive unit and integration tests to validate cryptographic implementations. Documented API usage and security considerations to ensure best practices and prevent common pitfalls in cryptographic development.

EDUCATION

Bachelor's Degree in Mathematics
University of Ilorin, Ilorin *Nov 2019 – Aug 2024*

- Conducted final-year research on: **"Natural Vibration Analysis of Axially Functionally Graded Tapered Rayleigh Beams Resting on a Bi-Parametric Elastic Foundation."**

PROJECTS

Sukura – Privacy-Focused Transaction Mixer
Jan 2025 – March 2025

- Built a privacy-focused transaction mixer for Solana using Groth16 zkSNARKs.
- Developed smart contracts with Anchor and implemented ZK circuits in Circom for anonymous transactions.
- Designed and built the frontend, integrating wallet connections and transaction workflows.

DeBook – Decentralized Book Platform
Jan 2025 – February 2025

- Built a decentralized book storage website, enabling censorship-resistant access to digital books.
- Integrated Cere blockchain to ensure secure and permanent book storage.
- Developed the frontend for a smooth user experience, including book uploads and retrieval.

ZK Word Mastermind Game – Zero Knowledge Puzzle Game
May 2025

- Built a two-player Mastermind-style word game leveraging zero-knowledge proofs for private guess validation.
- Implemented Cairo contracts and ZK circuits to verify hit/blow results without revealing the secret word.
- Integrated Starknet smart contracts with a dynamic React frontend for seamless proof generation, submission, and game flow.
- Ensured full on-chain privacy using zk-friendly logic for word comparison and player turns.

Obscura – Shielded Pool on Starknet
June 2025 - July 20205

- Developed a privacy-focused shielded pool for Starknet enabling confidential deposits, transfers, and withdrawals using zero-knowledge proofs over a UTXO-based model.
- Implemented Cairo contracts for shielded pool logic, Merkle tree commitments, and nullifier checks to prevent double-spends.
- Built Noir circuits with Honk proving for on-chain ZK verification and integrated Garaga-generated verifier contracts.
- Created a React + Vite frontend to handle encrypted transactions, proof generation, and seamless Starknet wallet interactions.
- Ensured full on-chain privacy using zk-friendly logic for word comparison and player turns.

ADDITIONAL INFORMATION

- **Open-Source Contributions**: Actively contribute to cryptographic and blockchain projects.
- **Technical Writing:** Writes documentation for various open-source projects.
- **Certifications & Workshops:** Engaged in blockchain security and cryptographic research communities.