

Arush Singh

SMART CONTRACT DEVELOPER

SOLIDITY & DEFI

github.com/04arush · linkedin.com/in/04arush
x.com/04arush · 04arush.github.io
04arush@gmail.com · New Delhi, India

PROFILE

Blockchain developer specialising in **Solidity smart contract** development, **DeFi protocols** and on-chain automation. Designed an intent-based batch auction exchange with **EIP-712** settlement, built a ZK-gated lending pool, and shipped a **Chainlink VRF & Automation** raffle. Grounded in contract security and rigorous **unit, fuzz and invariant testing** with Foundry.

SKILLS

Smart Contracts & Blockchain

Solidity Foundry DeFi OpenZeppelin Chainlink VRF / Automation / Oracle
Viem / Wagmi

Security & Testing

Slither Unit / Fuzz / Invariant Testing Echidna CodeHawks Ethernaut
CI Workflows

Protocol, ZK & Cryptography

Rust (arkworks) Go (Cosmos SDK) Noir (bb) Circom Groth16 / SNARKs STARKs
PLONK Poseidon Merkle Sum Trees Tokio Alloy

Languages & Tooling

TypeScript Node.js React Linux / Shell Git SQL (PostgreSQL) NoSQL (MongoDB)
Python

EXPERIENCE

Blockchain Protocol Engineer

Oct 2026 - Present

Cubane · Hybrid · Part-time

[Tech used: Rust · Go · Solidity · Noir · TypeScript]

- ▶ Design and develop scalable blockchain architecture for Cubane's platform, working directly with the founders and the product and design teams.
- ▶ Build secure smart contracts, decentralised protocol components and off-chain integrations.
- ▶ Monitor and optimise protocol performance for efficiency, security and reliability.

PROJECTS

Intent-Based Batch Auction Exchange

↗ GitHub

Solidity · Foundry · OpenZeppelin · Slither · CI

- ▶ On-chain spot exchange where traders sign **EIP-712** orders off-chain and an allowlisted solver submits them per **epoch**; the contract settles every trade **atomically at one uniform clearing price** that it computes itself.
- ▶ Solver supplies only sorted, signed orders. The contract picks the price, allocates fills by priority, and rounds buyers up and sellers down, sending dust to the treasury.
- ▶ Internal-escrow design: settlement makes **no token transfers or untrusted calls**, removing reentrancy risk. Owner has no function to move or freeze balances.
- ▶ Defence in depth with limit and conservation checks, nonce burning, ERC-1271 wallet support, and fee-on-transfer rejection.

ZK Undercollateralized Lending Protocol

➤ [GitHub](#)

Noir · Solidity · Foundry · OpenZeppelin · Next.js

- ▶ Undercollateralized lending (**50% collateral** vs the usual 150%):
LendingPool.borrow() verifies a Noir credit proof through a Barretenberg verifier before checking collateral and moving funds.
- ▶ Pool implements deposit, borrow, repay and liquidate with ReentrancyGuard, SafeERC20, strict naming conventions and full NatSpec.
- ▶ **100% line, branch and function coverage** across 23 tests: unit, fuzz, and invariant (128,000 actions per invariant) enforcing solvency, accounting integrity and collateral floors.

Provably Fair Raffle

➤ [GitHub](#)

Solidity · Foundry · Chainlink VRF v2.5 · Chainlink Automation

- ▶ Autonomous raffle with no admin intervention: **Chainlink Automation** triggers upkeep after each interval and **Chainlink VRF v2.5** selects a provably random winner, who receives the full pool before the raffle resets.
- ▶ Chain-aware deploy scripts via HelperConfig that also create, fund and register the VRF subscription.
- ▶ unit plus fuzz testing of state transitions and access control; deployed to Sepolia.

HACKATHONS

ETHOnline 2026

Participation Award

Built **StreamProof**, a private royalty-tier verification protocol: a Noir circuit (Poseidon2 Merkle inclusion + threshold proof) verified on-chain via UltraHonk on Arc Testnet.

Frostbyte Hackathon

Finalist · Participation Award

Qualified with the **Employee Payroll Manager** (Chainlink Automation), then advanced to the finale with the **ZK lending protocol**.

EDUCATION

Bachelor's — Computer Application

Aug 2023 - Ongoing

Indira Gandhi National Open University (IGNOU)
New Delhi, Delhi, IN

CERTIFICATIONS

Noir Programming & ZK Circuits	Cyfrin Updraft · Apr 2026
Fundamentals of Zero-Knowledge Proofs	Cyfrin Updraft · Mar 2026
Advanced Foundry	Cyfrin Updraft · Mar 2026
Foundry Fundamentals	Cyfrin Updraft · Mar 2026
Rust Programming Basics	Cyfrin Updraft · Feb 2026
Solidity Smart Contract Development	Cyfrin Updraft · Jan 2026
Blockchain Basics	Cyfrin Updraft · Dec 2025