

Bhavya Jain

Smart Contract & DeFi Security Engineer · Solidity · Foundry · EVM

Portfolio: bhavyajain-portfolio-blond.vercel.app

bhavyajain0718@gmail.com | github.com/bhavyajain0718-design | linkedin.com/in/bhavya-jain-7aa2522b4 | Jaipur, India

SUMMARY

Solidity engineer who ships and breaks DeFi contracts. Built and deployed ERC-1155 marketplaces, an over-collateralized lending market, Chainlink-integrated protocols and AMM clones — each hardened with CEI ordering and Foundry fuzz/invariant suites. Reproduces real exploit classes (reentrancy, oracle manipulation, flash-loan abuse, broken access control) and publishes them as formal audit-style findings. Targeting smart contract security and protocol engineering roles on L2 teams.

SMART CONTRACT SECURITY

Attack Vectors: Reentrancy (single, cross-function, read-only) · Flash-Loan Price Manipulation · Oracle Manipulation · Broken Access Control · Signature Replay · Delegatecall Hijacking · Front-Running / Sandwich · Griefing & DoS

Defensive Patterns: Checks-Effects-Interactions · Pull-over-Push Withdrawals · OpenZeppelin `AccessControl` · Slippage & Deadline Guards · Timelocks & Multisig · Safe Upgrades (UUPS / Transparent Proxy)

Methodology: Foundry invariant testing with handler-based fuzzing · Slither static analysis · Manual review against post-mortems of real exploits (Euler, Nomad, Ronin) · Gas-griefing and sequencer trust assumptions in L2 / Arbitrum environments

TECHNICAL SKILLS

Languages & Contracts: Solidity, TypeScript, Python, Node.js

Web3 Tooling: Foundry (forge, cast, anvil), Hardhat, OpenZeppelin, Slither, Chainlink (VRF v2, Price Feeds, Automation), Etherscan Verification, Sepolia

Standards: ERC-20, ERC-721, ERC-1155, EIP-712 Typed Signing, IPFS & On-Chain Metadata

App Layer: React 19, wagmi v3, viem, Express.js, PostgreSQL, MetaMask / WalletConnect, pnpm monorepo

ML / Research: PyTorch, YOLOv8-v11, RF-DETR (ViT), OpenCV

EXPERIENCE

Research Intern — Object Detection for Surgical Robotics May 2026 – Jun 2026
King's College London — Dept. of Informatics (Supervisor: Dr. Yang Li) London, UK

- Benchmarking CNN detectors (YOLOv1-v11) against transformer architectures (RF-DETR, Mask R-CNN) for robot detection in operating-theatre video, evaluated on mAP, inference latency and robustness under occlusion.
- Curated and labeled a custom surgical-scene dataset, fine-tuned both model families, and presented comparative findings in bi-weekly research meetings alongside a final written report.

Web3 Engineering Intern — Tokenized Real Estate Feb 2026 – Mar 2026
RentVerse · [GitHub] / RentVerse-Tokenized-Real-Estate Remote

- Architected and shipped 3 production Solidity contracts (ERC-1155 property listing, P2P marketplace, rent distributor) to Ethereum Sepolia, source-verified on Etherscan.
- Enforced Checks-Effects-Interactions ordering across every state-changing function with layered `ReentrancyGuard` + `Ownable`; Foundry unit and fuzz suites covering all core logic paths caught reentrancy and rounding edge cases pre-deployment.
- Built the wallet layer with wagmi v3 + viem — MetaMask/WalletConnect flows for on-chain investment, resale and transfer — plus a dynamic NFT metadata service (Node/Express) driving per-token URIs from live property state.

Quantitative Research Intern Jun 2025
Divya Capital One Pvt. Ltd. India

- Backtested algorithmic trading strategies and studied derivatives pricing, order-book microstructure and volatility modeling — the same mechanics that govern AMM pricing, liquidations and MEV.

SELECTED PROJECTS

Over-Collateralized Lending Protocol | Solidity, Foundry, Fuzz Testing [GitHub] / Lending-Borrowing-DeFi

- Deposit-ETH / borrow-CORN lending market enforcing a 120% minimum collateralization ratio on-chain at all times, with liquidation logic stress-tested against price-drop and partial-repay scenarios.
- Invariant suite asserts protocol solvency (total collateral value $\geq$ total debt) holds under randomized deposit, borrow, repay and liquidate sequences.

Security Lab — Exploit Reproductions | Solidity, Foundry, Slither [GitHub] / Codehawks-Security-Portfolio

- Published a formal security review of `PasswordStore` (access-control and on-chain data-privacy findings) structured as a professional audit report: severity classification, proof-of-concept, root cause, recommended mitigation.
- Rebuilding historical DeFi exploits from scratch — reentrancy chains, flash-loan-funded oracle manipulation, governance capture — each reproduced as a failing Foundry test before the fix is written.

Smart Agent Trading Bot | Solidity, Foundry, React 19, Node.js, PostgreSQL [GitHub] / AI-agent-trading-bot

- Autonomous trading agent ingesting live Kraken market data, scoring RSI/EMA/volatility signals and emitting an auditable reasoning trace before every trade; settlement executes on-chain via Solidity contracts verified on Sepolia. Typed pnpm monorepo — React 19 frontend, Express/PostgreSQL backend, wallet-scoped MetaMask sessions, Foundry-gated contract changes.

Decentralized Lottery | Solidity, Foundry, Chainlink VRF v2 + Automation [GitHub] / Decentralized-Lottery-Protocol

- Provably fair draw using Chainlink VRF for verifiable randomness and Automation for trustless scheduling; tested failure modes including callback reverts, upkeep starvation and payout griefing.

Also: Uniswap V2/V3 & Curve Stableswap AMM clones, collateral-backed stablecoin with invariant tests, [price-feed crowdfunding](#), [static & dynamic NFTs](#). 15 public repos.

EDUCATION

The LNM Institute of Information Technology (LNMIIT)
B.Tech-M.Tech (Dual Degree), Electronics & Communication Engineering

Jaipur, India
Expected 2028