

Preet Singh

📞 +91 79869 16377 ✉ preetsinghmakkar154@gmail.com 🌐 preet-singh 📄 preetsinghmakkar

PROFESSIONAL SUMMARY

Protocol Engineer with **2 years** of experience building and securing high-value DeFi and smart contract systems. Expert in upgradeable proxy architectures, invariant-driven design, fuzz and formal verification testing, and production-grade Solidity. Hands-on experience across full DeFi protocol stacks — from lending and AMMs to cross-chain stablecoin infrastructure on Cosmos SDK.

EXPERIENCE

Blockchain Developer

Feb 2026 – Present

iTechnolabs

- Architecting production-grade smart contracts powering tokenized financial systems with upgradeable UUPS and TransparentUpgradeableProxy patterns, preserving `--gap[50]` storage slots across all contracts
- Built **FollowMe Core** (NDA) — 9-contract on-chain brand management protocol enforcing a global ledger invariant (`available + staked + escrowed + excess == totalCredited - totalSpent - totalPenalties`) on every state mutation via a custom `enforceInvariant` modifier; 150-test Foundry suite spanning unit, integration, invariant, fuzz, and precision tests
- Implemented ERC20/ERC4626 tokenomics, role-based access control (6 distinct roles), vesting, linear settlement engines, and inactivity penalty systems with basis-point arithmetic verified across the full BPS range

Web3 Security Researcher — [Code4rena @RaOne](#) | [Cantina @RaOne](#)

Feb 2025 – Aug 2025

Code4rena · Cantina · Sherlock | \$391 earned · 1 High · 4 Medium · All-time rank #1593 on Code4rena

- Audited DeFi, lending, AMM, and agent protocol architectures; identified critical vulnerabilities across fund loss, access control bypass, DoS, and missing slippage/deadline protection vectors
- Virtuals Protocol** (High, #25): `PublicContributionNft::mint` is public with no access control, enabling arbitrary NFT minting and cascading fund loss across the contribution system
- Virtuals Protocol** (Medium): Attacker can permanently block execution of applications registered via `initFromToken()` in `AgentFactoryV4` by front-running registration
- Silo Finance** (Medium, #14): `deposit()`, `withdraw()`, and `redeem()` lack slippage bounds and deadline parameters, exposing users to sandwich attacks and stale execution
- Liquid Ron** (Medium, #12): Flawed `onlyOperator` modifier logic causes DoS for all authorized operators across critical protocol functions
- Aegis.im YUSD (Cantina)**: Undercollateralization via shared asset accounting — multiple positions drawing against the same underlying, enabling protocol insolvency
- Jigsaw Protocol (Cantina)**: Non-liquidatable undercollateralized positions due to missing health-factor checks in the repayment path, permanently locking bad debt

Full Stack Blockchain Engineer

Dec 2024 – Feb 2025

Ungate.io

- Engineered secure wallet infrastructure for controlled on-chain execution across multiple EVM-compatible networks; implemented strict authorization, signing validation, and failure-resilient transaction lifecycle management

PROJECTS

RevvFi Protocol | *Solidity, Foundry, Chainlink*

- Peer-to-peer DeFi lending protocol with multi-market architecture, competitive APR offer matching (lowest-APR-first, seniority-prioritized), and Dutch auction liquidation (5% hourly decay, 80% reserve price) with Chainlink oracle integration and 2-hour staleness detection
- Designed ERC721 lender position NFTs, epoch-based 7-day withdrawal queues preventing bank-run scenarios, and on-chain reputation scoring (0–1000, AAA–D labels) with +1 per repayment and -50 per default

Vesper Interchain | *Cosmos SDK, Go, Solidity, IBC, Ethermint*

- Sovereign Cosmos SDK blockchain bridging IBC-native collateral (stATOM, ATOM, stOSMO) with EVM DeFi; users deposit via IBC and mint USDx — an overcollateralized ERC20 stablecoin usable with MetaMask and Uniswap
- Designed a Solidity precompile at `0x000...0840` exposing the `x/collateral` module to EVM (200x faster than wrapped tokens); implemented 150% collateral ratio, keeper liquidations with 10% discount, and 5% APY stability fee

TECHNICAL SKILLS

Languages: Solidity, Go (Golang), Rust, TypeScript

Blockchain & Protocols: ERC20, ERC721, ERC4626, UUPS Proxy, TransparentUpgradeableProxy, Cosmos SDK, IBC, Ethermint, Chainlink Oracles

Security & Testing Tools: Foundry (forge fuzz, invariant), Hardhat, Slither, Echidna, Aderyn, Halmos (formal verification)