Dharmil Shah

Software Engineer | Applied AI, Backend & Blockchain

dharmilcv@gmail.com | github.com/trailofblocks | LinkedIn

Builds AI evaluations, payment workflows, resilient data services, and Solidity smart contracts. Production experience includes automated liquidity management and cross-network integrations.

Professional Experience

Steer Protocol | Solidity Lead Developer

Deployed and maintained 1,000+ smart contracts across 30+ networks, integrating with React, backend services, and on-chain indexing. Contributed to automated liquidity management that supported about $50M in peak protocol TVL and $1B+ in cumulative transaction volume.

SoluLab | Senior Blockchain Developer

Progressed from intern to senior developer. Built a 16-endpoint Node.js API with JWT authentication, MongoDB, and Web3 integrations. Implemented a cross-network bridge with WebSocket relayers and tested contracts using Hardhat and Ethers.js.

Smart Contract & DeFi Projects

Structured ERC-4626 Yield and Risk-Tranching Protocol | Built senior and junior vaults with a four-layer loss waterfall backed by curator bonds, junior capital, and independent cover pools. Built a React risk dashboard and deployed on Base Sepolia. Passed 105 Foundry tests, including stateful invariants, and formally verified selected properties.

Asynchronous Policy-Controlled Pooled Vault | Built pooled deposits, pro-rata shares, NAV accounting, and delayed ERC-7540 redemptions. Restricted keeper execution through Safe or ERC-4337 accounts. Passed 104 vault tests covering multi-user flows, NAV changes, and ERC-7540 compatibility.

Hybrid AMM and External Settlement Hook | Built a Uniswap V4 hook for hybrid or fully external collateral and stablecoin settlement. Enforced signed quotes, oracle deviation limits, per-block caps, and exact post-swap settlement using transient storage.

Scalable Automated Liquidity-Management Infrastructure | Designed a Beacon proxy upgrade architecture for hundreds to thousands of vaults across Uniswap V3/V4 and Algebra. Built persistent and just-in-time hooks that moved capital between V4 positions and ERC-4626 yield vaults.

Automated Carry-Trade Vault | Built an upgradeable ERC-4626 vault with allocator-managed borrowing and hard loan-to-value limits. Implemented proportional exits, strategy unwinds, fee accounting, and oracle and slippage safeguards.

Portfolio Projects

hometurf | Built a benchmark from repository bug fixes with tests that fail before each fix and pass afterward. Validated 32 tasks on sqlparse and compared solve rate, runtime, and cost.

AI Release Gate | Built a Python CI gate for refund assistants. The first policy candidate made six unsafe approvals. A corrected candidate passed all 48 labeled cases.

Treasury Change Control | Built a Safe transfer review desk that binds approval to the exact transaction hash. Verified two-owner execution on Anvil and hash parity through a read-only Sepolia check.

Online PostgreSQL Migration Kit | Built a Go migration kit with checkpointed backfills and rollback. The local benchmark handled 4,658 writes with zero failures or record mismatches.

Dispute Evidence Desk | Built a Stripe sandbox workflow that deduplicates delivery events, resumes after interruption, and exports a cited evidence packet after independent review.

Portfolio Projects continued

Allowance | Enforced recipient allowlists, periodic budgets, and co-signing through an ERC-7579 module, TypeScript SDK, and MCP server for x402 payments.

Reorg-Safe Blockchain Indexer | Built an ERC-20 indexer that replaces stale transfers atomically. Recovered from a three-block reorg and outage with 8 of 8 balance checks matching the chain.

Scope Search | Built cited workspace search with FastAPI and PostgreSQL row-level security. Verified that revoked access disappears from results, citations, and direct document requests.

MCP Airlock | Built a policy proxy for MCP tools with pinned definitions, source tracking, and an approval queue. The defensive lab blocked all seven synthetic unsafe cases.

agent-crashtest | Simulated lost replies, duplicate calls, and other faults for scripted agents. Checked committed effects across 117 single-fault runs to detect repeated or lost work.

Proof-of-Exploit | Built a defensive review workflow that independently verifies reported Solidity findings and checks proposed repairs against the original issue and regression tests.

Payment Risk Feature Store | Served live risk features from Kafka and PostgreSQL while retaining point-in-time snapshots through late events, duplicate deliveries, and worker restarts.

Canary Release Lab | Used Kubernetes, Argo Rollouts, and Prometheus to promote a healthy checkout release and abort a faulty one. Verified 50+ successful requests after rollback.

Payment Reconciliation Workbench | Built a finance workbench that matches processor records to bank settlements. A synthetic run turned 500 deliveries into 400 unique ledger entries.

Incident Replay Lab | Replayed logs, metrics, and traces to test incident hypotheses against cited evidence. The local model and rules engine passed all 12 synthetic checks.

Voyar Flight Search | Built a React and FastAPI flight planner that compares flexible dates and nearby airports, ranks price against travel time, and checks optional self-transfer layovers.

Continuation 095 | Used AI-assisted parameter sweeps and multi-period backtests to select a Nifty 500 momentum strategy. Modeled fees, slippage, and circuit limits across 1,741 simulated trades.

Strat Deck | Built an AI-assisted stock dashboard for strategy refreshes, holdings, orders, returns, and drawdown. The public edition passed 20 filing Q&A and 10 abstention checks.

Technical Skills

Languages and application stack | Solidity, JavaScript, TypeScript, Python, Go, React, Node.js, FastAPI, MongoDB, PostgreSQL, SQLite

AI and infrastructure | LLM evaluation, citation-backed RAG, Claude API, Ollama, MCP, Kafka, Docker, Kubernetes, Argo Rollouts, Prometheus, GitHub Actions

Smart contract tooling | Foundry, Hardhat, Truffle, Ethers.js, Viem, Web3.js, OpenZeppelin

Protocols and standards | Uniswap V3/V4, Algebra, Liquity, ERC-20, ERC-721, ERC-1155, ERC-4626, ERC-6909, ERC-7540, ERC-4337, ERC-7579, x402

DeFi and architecture | Automated liquidity management, concentrated liquidity, structured products, lending and borrowing, collateral settlement, policy-controlled execution, Safe and Kernel accounts, Beacon and UUPS proxies

Testing and security | Unit, fork, fuzz, and invariant testing, Aderyn, Halmos, Yices SMT Solver, Slither, MythX, pytest, Playwright, oracle, slippage, and access-control safeguards

Networks | Ethereum, Base, Arbitrum, Optimism, Polygon, BNB Smart Chain, and other EVM-compatible networks

Education

B.Tech. in Information Technology | Indus University | 2021