VibeSwap Build Summary

What it is: Omnichain DEX on LayerZero V2 that eliminates MEV through commit-reveal batch auctions with uniform clearing prices.

Philosophy: Cooperative Capitalism — mutualized risk (insurance, treasury stabilization) + free market competition (priority auctions, arbitrage).

Codebase: 121 Solidity contracts | 119 test files | 859+ tests passing | 51 frontend components | 14 hooks | 5 deploy scripts

---

Tech Stack

- **Contracts:** Solidity 0.8.20, Foundry, OpenZeppelin v5.0.1 (UUPS upgradeable)
- **Frontend:** React 18, Vite 5, Tailwind CSS, ethers.js v6
- **Oracle:** Python 3.9+, Kalman filter for true price discovery
- **Cross-chain:** LayerZero V2 OApp protocol
- **Deployed:** Vercel (frontend), testnet prep in progress

Core Mechanism — 10-Second Batch Auctions

- **Commit Phase (8s):** Users submit `hash(order || secret)` with deposit
- **Reveal Phase (2s):** Reveal orders + optional priority bids for execution ordering
- **Settlement:** Fisher-Yates shuffle using XORed secrets, uniform clearing price for all trades in the batch
- **Result:** No MEV extraction possible — all users get the same price, order sequence is unpredictable

---

Layer 1: Core Protocol (Phase 1)

Trading Engine

- **CommitRevealAuction** — Batch auction mechanism with commit/reveal/settle lifecycle
- **VibeAMM** — Constant product AMM (x*y=k) with TWAP oracle, protocol fees, emergency pause
- **VibeSwapCore** — Main orchestrator connecting auction, AMM, and cross-chain
- **VibeLP** — ERC-20 LP token for liquidity positions

Cross-Chain

- **CrossChainRouter** — LayerZero V2 messaging for omnichain swaps, peer management, rate limiting, replay prevention, bridged deposit expiration (24h)

Security Infrastructure

- **CircuitBreaker** — Volume, price, and withdrawal threshold triggers
- **SecurityLib** — Signature verification, nonce management
- **Flash loan protection** — EOA-only commits
- **TWAP validation** — Max 5% deviation from oracle price
- **Rate limiting** — 1M tokens/hour/user
- **50% slashing** — For invalid reveals (game-theoretic enforcement)

Libraries

- **DeterministicShuffle** — Fisher-Yates using XORed trader secrets
- **BatchMath** — Uniform clearing price computation
- **TWAPOracle** — Time-weighted average price tracking
- **VWAPOracle** — Volume-weighted average price
- **TruePriceLib** — Price aggregation utilities
- **PairwiseFairness** — On-chain fairness verification for conviction voting
- **IncrementalMerkleTree** — Hybrid Eth2/Tornado Cash/OZ Merkle tree (gas-efficient inserts, root history ring buffer, OZ proof compatibility)

Layer 2: Financial Primitives (10/10 Complete)

1. **wBAR** — Wrapped Batch Auction Receipts (tokenized auction positions)
2. **VibeLPNFT** — ERC-721 LP position manager wrapping VibeAMM; full lifecycle: mint, increase, decrease, collect, burn; two-step withdrawal; TWAP entry price
3. **VibeStream** — Token streaming (linear vesting) + FundingPool mode with conviction voting (stake x time), lazy evaluation, on-chain pairwise fairness
4. **VibeOptions** — European-style calls/puts as ERC-721 NFTs; fully collateralized by writer; cash-settled via TWAP; Black-Scholes premium suggestion
5. **Joule (JUL)** — Trinomial Stability Token: RPow mining (SHA-256 PoW anchoring value to electricity cost), PI controller rebase targeting, elastic supply with equilibrium band; custom ERC-20 with O(1) rebase via global scalar
6. **VibeBonds** — Fixed-rate bond issuance and settlement
7. **VibeCredit** — Under-collateralized credit lines with trust-weighted limits
8. **VibeSynth** — Synthetic asset creation and tracking
9. **VibeInsurance** — Mutual insurance pools with coverage and claims
10. **VibeRevShare** — Revenue sharing distribution to stakeholders

---

Layer 3: Protocol Framework (10/10 Complete)

1. **VibeHookRegistry** — Pluggable hook system for extending pool behavior at defined points (beforeSwap, afterSwap, etc.)
2. **VibePluginRegistry** — Plugin management with versioning and dependency tracking
3. **VibeKeeperNetwork** — Decentralized keeper system for automated maintenance tasks (liquidations, rebalancing, oracle updates)
4. **VibeForwarder** — ERC-2771 meta-transaction forwarder for gasless UX
5. **VibeSmartWallet** — Account abstraction wallet with session keys and spending limits
6. **VibeWalletFactory** — Deterministic smart wallet deployment
7. **VibeVersionRouter** — Proxy router for contract upgrades without migration
8. **VibePoolFactory** — Modular pool creation with pluggable curves (ConstantProduct, StableSwap with Curve.fi invariant); permissionless; deterministic IDs; hook integration
9. **VibeIntentRouter** — Intent-based order routing: users say "swap X for best Y", router quotes AMM, factory pools, batch auction, cross-chain and picks optimal
10. **VibeProtocolOwnedLiquidity** — Treasury-owned LP positions earning fees perpetually; self-sustaining flywheel

---

Layer 4: Governance & Compliance

Governance

- **DAOTreasury** — Protocol fee collection, backstop liquidity (95% slippage protection), timelock proposals
- **TreasuryStabilizer** — Automated rebalancing of treasury assets
- **VibeTimelock** — Time-delayed execution for governance proposals
- **DecentralizedTribunal** — On-chain dispute resolution with juror staking (pull-pattern settlement, Sybil-resistant via SoulboundIdentity)
- **DisputeResolver** — Arbitrator assignment and case management (bounded loops for gas DoS prevention)
- **AutomatedRegulator** — Rule-based automated compliance enforcement

Governance Mechanisms

- **QuadraticVoting** — Square-root weighted voting to reduce plutocracy
- **CommitRevealGovernance** — Secret ballot governance (same commit-reveal pattern as trading)
- **ConvictionGovernance** — Time-weighted continuous signaling

Compliance

- **ComplianceRegistry** — KYC/AML tracking with expiry checks
- **FederatedConsensus** — Multi-authority consensus for compliance decisions (min 2 authorities)
- **ClawbackRegistry** — Regulatory clawback case management (bounded at 1000 wallets/case)
- **ClawbackVault** — Frozen asset custody with release controls (zero-address protection)

Layer 5: Identity & Incentives

Identity

- **SoulboundIdentity** — Non-transferable identity tokens; recovery via 2-day timelock
- **ContributionDAG** — On-chain trust DAG (Web of Trust); BFS trust scores from founders with 15% decay/hop (max 6 hops); vouches, handshakes, referral quality, diversity scores; Merkle-compressed vouch audit trail
- **GitHubContributionTracker** — Webhook-driven GitHub ingestion via EIP-712 signed relayers; Merkle-compressed; records commits, PRs, reviews, issues as verifiable contributions
- **Forum** — On-chain discussion with SoulboundIdentity-signed posts
- **WalletRecovery** — Social recovery with guardian threshold validation
- **AGIResistantRecovery** — Future-proof recovery mechanisms

Incentives

- **ShapleyDistributor** — Game-theoretic reward distribution using Shapley values
- **RewardLedger** — Retroactive + active Shapley rewards; dual-mode: pre-launch retroactive claims + real-time trust-chain-weighted distribution; efficiency axiom: all value fully distributed
- **ContributionYieldTokenizer** — Pendle-inspired tokenization: Idea Tokens (instant full-value, never expire, instantly liquid) + Execution Streams (conviction-voted, stale decay, redirectable)
- **PriorityRegistry** — Priority bid tracking for auction ordering
- **LoyaltyRewardsManager** — Long-term user reward programs (fee-on-transfer safe)
- **SlippageGuaranteeFund** — Slippage compensation pool (configurable daily limits)
- **ILProtectionVault** — Impermanent loss protection for LPs
- **ReputationOracle** — On-chain reputation scoring

Market Mechanisms

- **BondingCurveLauncher** — Token launch via bonding curves
- **PredictionMarket** — Binary outcome prediction markets
- **DutchAuctionLiquidator** — Dutch auction for liquidation events
- **HarbergerLicense** — Harberger tax licensing for scarce resources
- **RetroactiveFunding** — Retroactive public goods funding rounds
- **CommitRevealAuction** (governance) — Sealed-bid auctions for governance

---

Layer 6: Advanced / Future-Proof

- **QuantumGuard** — Post-quantum signature verification framework
- **QuantumVault** — Quantum-resistant asset storage (key exhaustion protection)
- **LamportLib** — Lamport one-time signature library
- **TruePriceOracle** — Multi-source price aggregation with Kalman filter
- **StablecoinFlowRegistry** — Stablecoin flow tracking with bounded ratios
- **VolatilityOracle** — Historical volatility computation
- **VolatilityInsurancePool** — Volatility event coverage (per-event claim tracking)

Frontend (51 Components)

Core Pages

- **SwapPage / SwapCore** — Token swap interface
- **BuySellPage** — Buy/sell with fiat on-ramp
- **PoolPage** — Liquidity provision interface
- **BridgePage** — Cross-chain transfers (0% protocol fees, only LayerZero gas)
- **RewardsPage** — Reward tracking and claims
- **ActivityPage** — Transaction history and activity feed
- **AnalyticsPage** — Protocol analytics and charts

Game-Like UX (Runescape Grand Exchange Feel)

- **TradingPost** — Main trading interface styled as a game trading post
- **GameSwapPage** — Gamified swap experience
- **Inventory** — Portfolio displayed as game inventory
- **LootChest** — Reward claiming as loot opening
- **PlayerStats** — User stats as player profile
- **SoulboundAvatar** — Identity-linked avatar
- **BatchTimer** — Visual countdown for batch phases
- **MarketMood** — Sentiment indicator

Identity & Social

- **ForumPage / MessageBoard** — Community discussion
- **ContributionGraph** — Trust DAG visualization
- **PersonalityPage** — User personality assessment
- **CreateIdentityModal** — Soulbound identity creation
- **OnboardingModal** — New user onboarding

Security

- **VaultPage** — Savings vault (hot/cold separation)
- **PaperBackup** — Offline recovery phrase backup
- **RecoverySetup** — Account protection configuration
- **WalletSafetyBadge** — Visual security status
- **QuantumVaultModal** — Quantum-safe storage interface

Wallet

- **Dual wallet support:** External (MetaMask etc.) + Device (WebAuthn/passkeys)
- **"Sign In" not "Connect Wallet"** — Abstracting away blockchain complexity
- Keys stay in user's Secure Element, never on servers

Security Posture

- **7 audit passes** completed across all contracts
- **35+ findings fixed** (8 critical, 12 high, 10 medium, 5+ low)
- Critical fixes: double-spend prevention, ETH refund on reveal, reentrancy guards, pull-pattern settlements, Sybil resistance
- **UUPS upgrade safety:** All 25 upgradeable contracts have `onlyOwner _authorizeUpgrade`
- **18 adversarial money path tests:** LP sandwich, first depositor, rounding theft, donation manipulation, double spend, slash accounting
- **22 security attack tests:** Flash loan, price manipulation, circuit breakers, reentrancy
- Cross-chain security parity: all 5 security modifiers applied to cross-chain paths

---

Test Coverage

Category	Tests
Unit tests	500+
Fuzz tests (256 runs each)	200+
Invariant tests (128K calls each)	130+
Integration tests	30+
Security/adversarial tests	40+
Game theory tests	20+

Total	**859+**

All tests passing. Zero failures. Zero skipped.

What's Next

- **Off-chain relayer service** for GitHub webhook ingestion
- **IPFS/Arweave integration** for Merkle tree data archival
- **Testnet deployment** (deploy scripts ready, verified)
- **Frontend redesign** — cypherpunk aesthetic, deeper game-like abstraction
- **Invariant tests** for GitHubContributionTracker, CrossChainRouter, wBAR, TruePriceOracle