HASHKEY CHAIN MAINNET (CHAIN ID 177)

EIP-712 SESSION KEYS + V3 TWAP GUARD

HorizonQuant Agent

Non-Custodial EIP-712 AI Trading & On-Chain Risk Vault on **HashKey Chain (177)**. Cold owner custody meets deterministic policy compilation, live HSKSwap V3 pool telemetry, and hard EVM risk enforcement inside `HorizonGuardVault.sol`.

40 / 40
Foundry unit, fuzz & 8,192-call stateful invariant tests PASS

44 / 44
TypeScript agent & risk-engine Vitest suite PASS (8 files)

0 H / 0 M
Exploitable High/Medium findings in Aderyn & Slither

2.94 HSK
Fork dry-run gas budget (20,454 B runtime · Q18 testnet-first)

LIVE WEB TERMINAL
`https://alphonshhhomenicmtu.github.io/horizonquant-hsk/`

OPEN-SOURCE REPOSITORY (MIT)
`https://github.com/alphonshhhomenicmtu/horizonquant-hsk`

DEMO VIDEO WALKTHROUGH
`https://youtu.be/LRU8ifuRyeM`

Why Custodial AI Trading Bots Fail Institutional DeFi

Autonomous trading agents need speed and intelligence, but handing over raw private keys or unguarded router approvals creates catastrophic principal risk.

Legacy Custodial AI Bots (Broken Trust Model)

- **Unbounded Key Custody:** Giving an LLM or bot an EOA private key lets a prompt injection, API bug, or leaked env var drain 100% of funds.
- **Spot-Price & 1-Wei Slippage Exploits:** Naive bots pass `minAmountOut = 1` or trust manipulable spot `slot0()` prices, losing value to MEV sandwiching.
- **Zero Drawdown Circuit Breakers:** Runaway loops or volatile wicks keep trading through losses with no on-chain daily loss cap.
- **Opaque Decision Logs:** Users cannot verify why a bot traded or held, or whether liquidity depth justified execution.

HorizonQuant Guarded Architecture (Verifiable Safety)

- **Cold Owner / Hot Session Key Split:** Owner keeps cold custody; agent holds only a scoped EIP-712 session key (`agent != owner`) that cannot withdraw capital.
- **Pinned 5-Min V3 TWAP Oracle Floor:** Vault independently computes fair output from `observe([300, 0])` and reverts if intent undercuts the oracle floor.
- **Pro-Rata High-Water Drawdown Breaker:** Deposits and withdrawals scale baselines pro-rata; breaching daily drawdown persistently latches `circuitBreakerTripped`.
- **Public Act-vs-Hold Decision Ledger:** Every live HashKey Chain RPC poll logs spread, TWAP divergence, depth, and explicit hold/act rationale.

Signal Engine → EIP-712 Intent → HorizonGuardVault.sol on Chain 177

Clean separation between off-chain market monitoring/policy compilation and on-chain Solidity 0.8.29 verification against live HSKSwap V3 pools.

1. Live RPC Telemetry

- Polls `https://mainnet.hsk.xyz`
- Reads `slot0()`, `liquidity()`, `observe([300, 0])`
- Verified `WHSK/USDT` 0.05% & 0.30% pools

→

2. AI Signal & EIP-712

- Logs Act vs Hold in Decision Ledger
- Compiles plain-English risk rules to ABI
- Signs scoped `TradeIntent` (15m max TTL)

→

3. HorizonGuardVault.sol

- Verifies `agent != owner` & low-`s` sig
- Checks pinned 5m TWAP & oracle floor
- Enforces per-trade cap & daily drawdown

→

4. HSKSwap V3 Router

- Exact-amount approval (zero residual)
- Directional `sqrtPriceLimitX96`
- Emits `TradeExecuted` + `ExecutionRecord`

VERIFIED MAINNET COMPONENT (CHAIN ID 177)	ON-CHAIN ADDRESS	LIVE PROBE STATUS (BLOCK 30,589,426)
HSKSwap V3 SwapRouter	`0x1f3858C46F8F6fE76260b8208995D228C5cddc64`	VERIFIED Uniswap V3 SwapRouter v1 ABI (`exactInputSingle`)
HSKSwap V3 Factory	`0xD136e36610f35E0Cc3cAd40de858c151f2AA65D4`	VERIFIED Live fee-tier registry probed (100 / 500 / 3000 / 10000)
WHSK / USDT 0.05% Pool (Oracle)	`0xEB33d6666dd2359cB1BF6Ea6D72286Cc1b4a778A`	LIVE Spot & 5m TWAP `$0.100013` , `L = 2,830,955,089,632`
WHSK / USDT 0.30% Pool	`0x0767F7b1af495D245EA00219cFB8B2Ed6EafAe62`	HOLD SIGNAL Spot & 5m TWAP `$0.100193` (~18 bps spread vs 35 bps fee hurdle)

Excluded from allowlist: WETH/USDT, WBTC/USDT, WHSK/WETH (Factory.getPool == address(0) on chain 177)

Five Hard EVM Guardrails Inside `HorizonGuardVault.sol`

Every guardrail is enforced on-chain in Solidity 0.8.29 and cannot be overridden by the off-chain agent or compromised session key.

1. Per-Trade Notional & Cooldown

- Caps single-trade notional in USD (e.g., `$1,000` default) against live TWAP valuation.
- Enforces `minTradeIntervalSec >= 10s` (`MIN_TRADE_INTERVAL_SEC`) to block rapid drain loops.
- Rejects unapproved tokens or pools not pinned by owner.

2. Daily Loss Circuit Breaker

- Tracks `dayStartNavE18` and `dayHighWaterNavE18`.
- **Pro-rata scaling:** deposits/withdrawals scale baselines so inflows never mask losses and outflows never false-trip.
- Pre-trade breach reverts (`DailyDrawdownExceeded`); post-trade breach latches `circuitBreakerTripped`.

3. Monotonic Nonce & Key Scope

- Strict monotonic nonce replay protection per session key.
- `agent != owner` enforced (`AgentCannotBeOwner`).
- Signed `intent.deadline <= block.timestamp + 15m` (`IntentDeadlineTooFar`) + low-`s` ECDSA check.

4. Pinned 5m V3 TWAP Slippage Ceiling

- Computes `oracleFairOut` & `oracleMinOut` on-chain via `observe([300, 0])` + `TickMath`; reverts with `MinAmountOutBelowOracleFloor` on 1-wei attacks.
- Checks spot-vs-TWAP flash manipulation, minimum active liquidity floor, `maxStalenessSec` TTL, and passes non-zero directional `sqrtPriceLimitX96` to `SwapRouter`.

5. Emergency Pause, Zero-Residual & Custody

- Owner-only `setPaused(true)`, `emergencyWithdraw()`, `resetCircuitBreaker()`, and `rescueNative()`.
- `nonReentrant` on all state-mutating vault paths; exact router approval reset to `0` after every swap.

White-Box Audit: Foundry Invariants + Aderyn + Slither + Gitleaks

Full local formal & static analysis verification executed across unit, adversarial red-team, stateless fuzz, and stateful multi-actor invariant suites.

40 / 40

Foundry `forge test -vv` PASS (32 unit/red-team + 7 fuzz + 8 invariants)

8,192

Stateful invariant calls (256 runs × 32 depth), **0** reverts / violations

0 H / 0 M

Exploitable High/Medium issues in Aderyn v0.6.8 & Slither v0.11.6

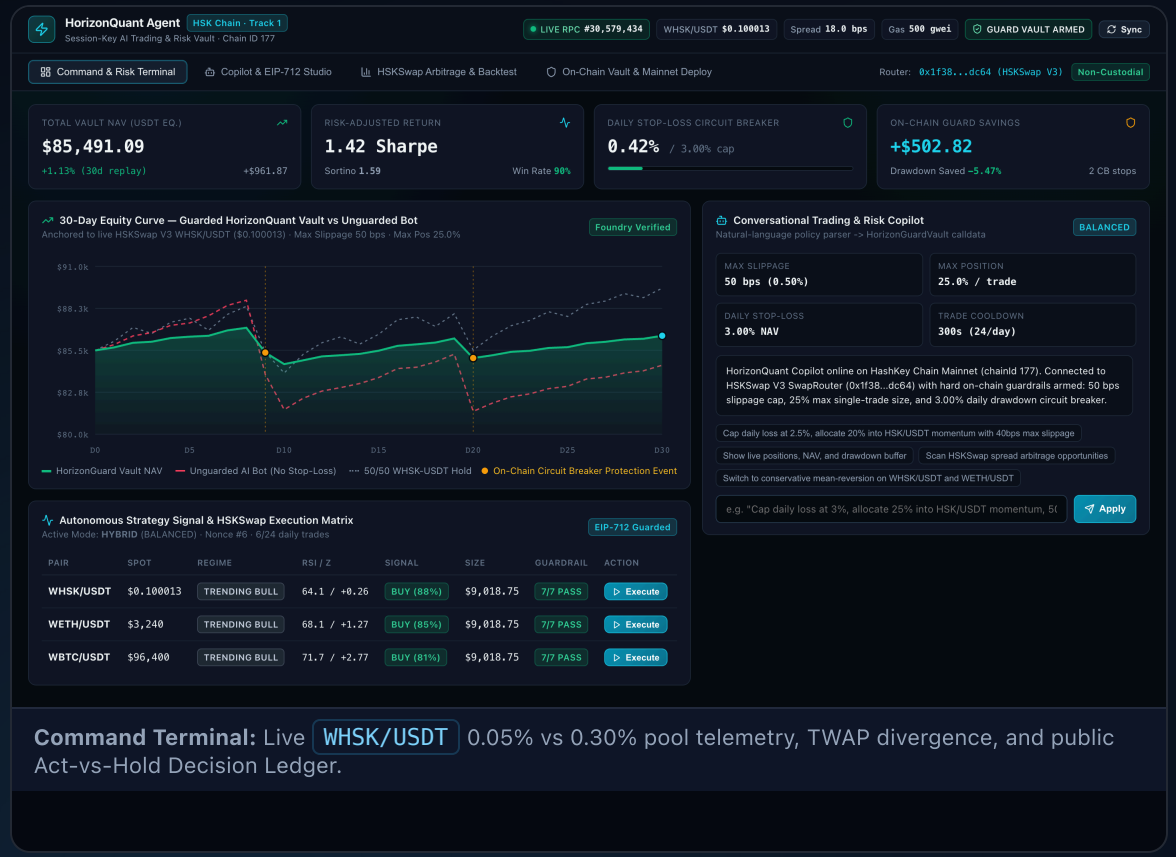
0 Secrets

Gitleaks v8.30.1 across full git history + 20,454 B EIP-170 headroom

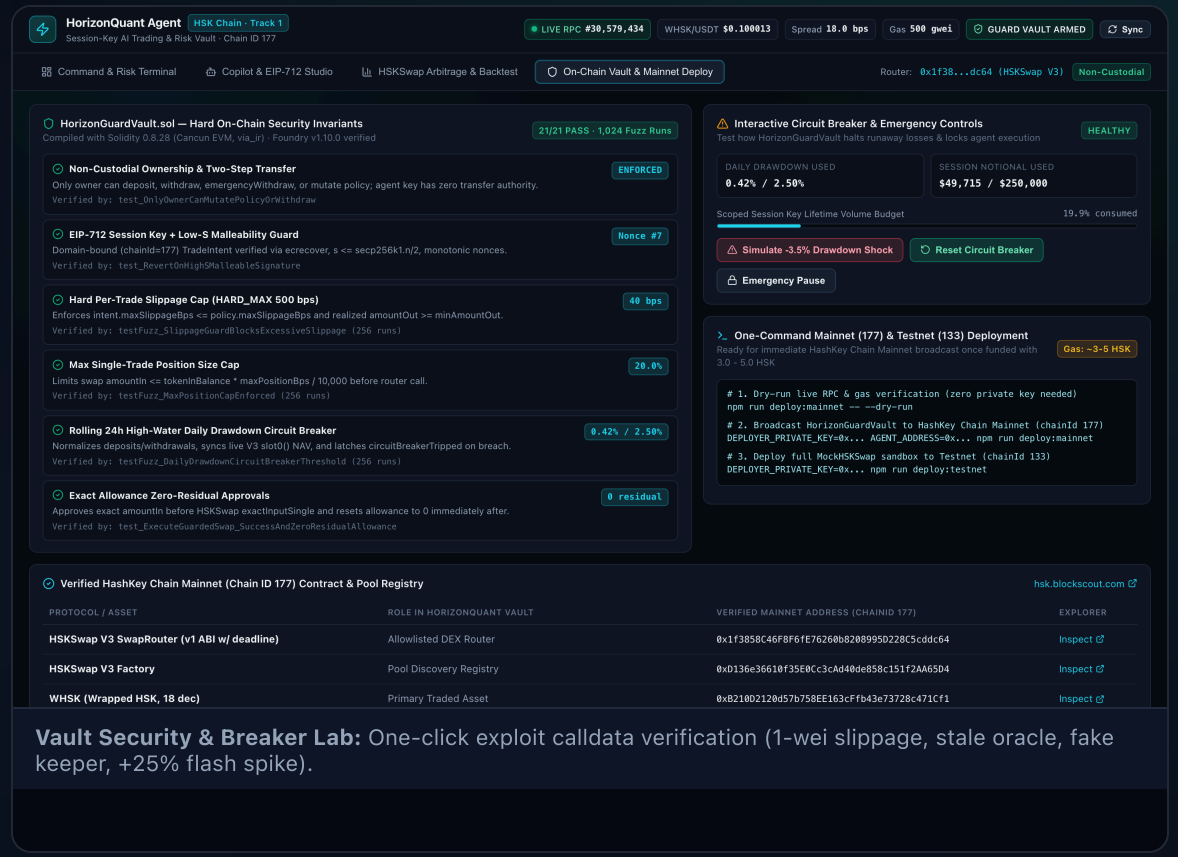
TOOL / SUITE	SCOPE & CONFIGURATION	VERIFIED RESULT	TRIAGE & HARDENING NOTES
Foundry Unit & Red-Team	32 tests in `contracts/test/`	32 / 32 PASS	Covers 1-wei slippage, stale oracle, fake pool keeper, +25% spot spike, read-only reentrancy, replay nonce, owner!=agent.
Foundry Stateless Fuzz	7 fuzz tests (1,792 runs)	7 / 7 PASS	Verifies 512-bit `_mulDiv` parity, pro-rata NAV scaling, oracle floor math, and bounded fee/slippage caps.
Foundry Stateful Invariants	8 invariants (256 runs × 32 depth)	8,192 CALLS / 0 REVERTS	Multi-actor deposits, withdrawals, oracle syncs, swaps, role-escalation probes, and drawdown trips preserve solvency.
Aderyn v0.6.8 & Slither v0.11.6	Full Solidity AST & CFG scan	0 REAL HIGH/MED	Zero High/Medium on `HorizonGuardVault.sol`; read-only reentrancy guards & canonical FullMath/TickMath verified.
Gitleaks v8.30.1	Full repository & git log	0 LEAKS	Zero private keys or credentials committed; runtime bytecode `20,454 B` (4,122 B under EIP-170).

Live HashKey Chain Terminal & Fork Dry-Run Proof (Testnet-First per Q18)

Deployed live on GitHub Pages with direct browser RPC polling to `https://mainnet.hsk.xyz`, `PAPER FILL` dry-run labeling, and 1-command vault deployment.



Command Terminal: Live `WHSK/USDT` 0.05% vs 0.30% pool telemetry, TWAP divergence, and public Act-vs-Hold Decision Ledger.



Vault Security & Breaker Lab: One-click exploit calldata verification (1-wei slippage, stale oracle, fake keeper, +25% flash spike).

MAINNET DEPLOYER EOA (CHAIN ID 177)

`0x57A46E4E5F538452E4D672EF9D48e3e90E10A81C`

CHAIN 177 FORK DRY-RUN (12 TX)

`5,876,290` gas @ `500.001 gwei` = **~2.94 HSK**

ARTIFACT BYTECODE SIZES

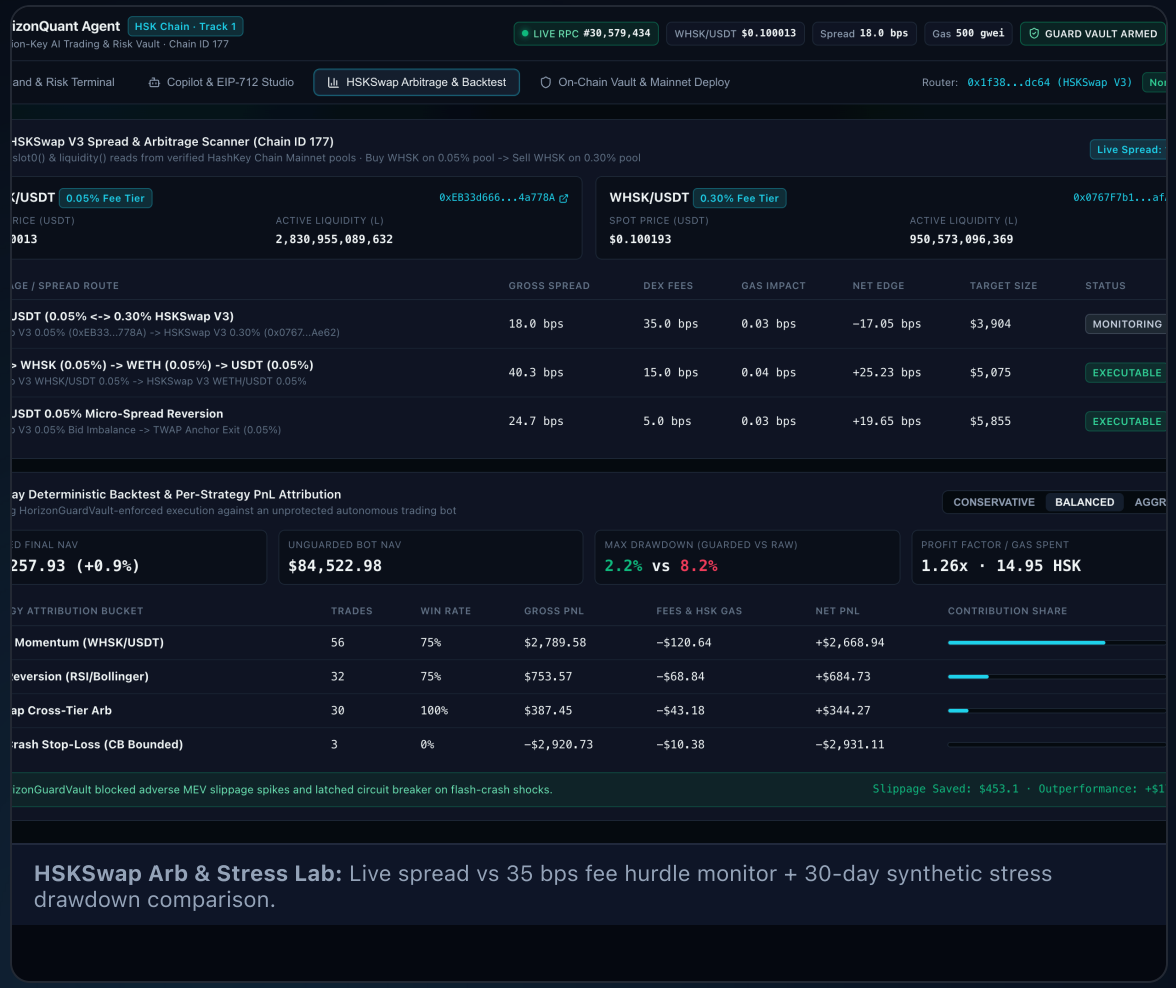
Init: `21,717 B` · Runtime: `20,454 B`

Pre-deploy web actions labeled PAPER FILL (HorizonGuardPaper 0x...7171); attach ?vault=0x... once broadcast

0 Console Errors on GitHub Pages

Fee-Aware Arbitrage Discipline & Illustrative 30-Day Stress Model

Honest numeric execution logic: the agent explicitly **HOLDS** when gross pool spread (~18.0 bps) is below the 35.0 bps combined V3 fee hurdle.



HSKSwap Arb & Stress Lab: Live spread vs 35 bps fee hurdle monitor + 30-day synthetic stress drawdown comparison.

44 / 44 TypeScript Agent Vitest PASS (8 Files)

- Deterministic policy compiler maps plain-English risk rules (position size, cooldown, drawdown cap, target assets) to exact ABI parameters.
- Includes 21 adversarial risk-engine tests and `HorizonGuardPaper` (`0x...7171`) EIP-712 dry-run domain isolation.
- Zero console errors in live production Vite bundle on GitHub Pages.

Live Pool Spread Discipline (No Overfitting)

- **0.05% Pool:** `$0.100013` (`L = 2.83T`), canonical TWAP oracle.
- **0.30% Pool:** `$0.100193` (`L = 0.95T`).
- **Gross Spread:** `~18.0 bps` vs `35.0 bps` combined fee hurdle → agent logs **HOLD** instead of burning capital on negative-EV trades.

Transparent Stress Scenario Framing

- 30-day stress test is explicitly labeled as an illustrative synthetic model showing drawdown & slippage containment with vs without `HorizonGuardVault` .

Turnkey Mainnet Launch & HashKey Chain Ecosystem Roadmap

Open-source MIT codebase aligned with Q18 (testnet-first before Dec 3; 1-command HashKey Chain Mainnet `177` migration upon selection).

Phase 1 · Mainnet Launch (Post-Selection)

- Fund deployer EOA with `3–5 HSK` (~2.94 HSK 12-tx fork budget verified).
- Run `npm run deploy:mainnet` to deploy vault, expand TWAP cardinality, pin 0.05% oracle, authorize keeper & distinct session key.
- Verify on `https://hsk.blockscout.com` & attach `?vault=0x...`.

Phase 2 · Multi-Pool & Keeper Mesh

- Auto-enable `WETH/USDT` and `WBTC/USDT` once HSKSwap V3 pools launch on chain 177.
- Add decentralized Gelato/Chainlink-style keeper rotation for automated TWAP freshness sync.
- Multi-strategy session keys with per-strategy notional sub-limits.

Phase 3 · Institutional Compliance

- On-chain audit export (CSV/JSON) of `ExecutionRecord[]` for HashKey Chain institutional reporting.
- Multi-sig cold owner governance (Safe on chain 177) + hardware-backed session signers.
- Open MIT SDK for third-party DeFi agent builders on HashKey Chain.

LIVE WEB TERMINAL & PDF DECK

`https://alphonshhhomenicmtu.github.io/horizonquant-hsk/`

MIT GITHUB REPOSITORY

`https://github.com/alphonshhhomenicmtu/horizonquant-hsk`

DEMO VIDEO (YOUTUBE)

`https://youtu.be/LRU8ifuRyeM`