

Hexa DEX - Whitepaper

Version 1.0 - October 2025

This document is informational and not investment, legal, or tax advice.

0. Executive Summary

Hexa DEX is a **privacy-first perpetual futures exchange** that hides trader intent until settlement while preserving on-chain verifiability post-trade. By combining **sealed order flow**, **frequent batch** matching, post-trade proofs, and a conservative risk engine, Hexa aims to neutralize stop-loss hunting, predatory liquidations, and MEV-based exploitation - and deliver fair execution for retail-pro and institutional traders alike.

The **\$HEXA token** is a true fair-launch asset with a fixed supply. 100% of protocol revenue is distributed to token holders in ETH pro-rata by wallet holdings. The protocol's operating budget comes solely from a 5% buy/sell tax; there are no KOL supply handouts and no OTC allocations.

Why now: leading derivatives DEXs have matured designs around matching, oracles, and liquidations, but continue to suffer from order-flow leakage and MEV exposure; at the same time, many token launches are structurally unfair and exploitative. Hexa addresses both: market-structure fairness and token-level fairness.

1. Problem & Vision

Public order flow in L1/L2 mempools reveals trader intent, enabling frontrunning/sandwiching, stop-loss hunting, and liquidation dynamics that erode PnL and confidence. Batch-auction and order-sealing mechanisms are known to dampen latency races and reduce extraction by aligning execution into discrete intervals with uniform-price auctions; secrecy before settlement, paired with verifiability after settlement, is the critical missing ingredient for on-chain perps.

Hexa's vision: an on-chain derivatives venue that keeps you private when it matters and proves integrity/compliance when it counts - without custodial risk.

2. Protocol Overview

Goals

- **Fair execution** via sealed orders and frequent batch auctions (FBA).
Orders are only revealed at settlement, eliminating front-running and intent leakage.
- **Verifiable integrity** via succinct post-trade proofs and auditable state commitments.
- **Robust risk controls:** mark-price based liquidations, partial de-risking, and a protocol-level backstop mechanism.
- **Non-custodial by design:** standardized, trustless deposit and withdrawal flows.

Key Concepts

- **Sealed order flow:**
Orders (including stop orders) are submitted in encrypted or committed form and remain opaque until batch closure. No pre-trade order details — such as price, size, or side — are exposed before settlement. Privacy is enforced by a distributed matching process that ensures no single party can reconstruct individual orders prematurely.
- **Frequent batch matching:**
Orders are aggregated into short time intervals (e.g., sub-second to multi-second batches). At the end of each batch, a uniform clearing price per market is determined by maximizing surplus while respecting constraints. This mechanism reduces front-running, minimizes latency races, and neutralizes MEV incentives.
- **Post-trade proofs:**
After each settlement, compact proofs and receipts are published to allow independent verification of fills and risk changes without revealing pre-trade

intent or individual order details. This preserves privacy while ensuring system integrity.

- **MEV-aware routing:**

All order submissions leverage privacy-preserving relayers and secure RPC layers. The protocol architecture supports governance-approved integrations with MEV-resistant execution builders or routers.

3. System Architecture

3.1 Order Lifecycle

1. **Intent capture**

User signs an order specifying price bounds, size, side, time-in-force, and optional stop/take-profit conditions.

2. **Order sealing**

Orders are encrypted or committed in a privacy-preserving epoch. Metadata leakage is minimized to avoid revealing intent or timing information.

3. **Batching & matching**

Orders enter a discrete batch window. A distributed matching process determines the uniform clearing price and produces per-account net changes. No participant learns other orders before settlement.

4. **Settlement**

Position states are updated on-chain or through a verifiable commitment to the latest state root. Funding payments are accrued, and realized PnL is computed.

5. **Proofs & receipts**

Compact proofs (e.g., cryptographic commitments) and receipts are published for each batch. These allow traders, auditors, and third parties to verify settlement integrity without leaking order-level detail.

3.2 Risk Engine

- **Mark price:** derived from a medianized oracle feed (blending multiple providers with freshness constraints).
- **Margins:** dynamic initial/maintenance margin levels per market, with cross/isolated margin modes on the roadmap.
- **Partial liquidation first:** positions are reduced proportionally to restore margin requirements before full liquidation.
- **Insurance/backstop:** a protocol-owned reserve and auction-based backstop mechanism ensures orderly liquidation in extreme conditions.

3.3 Oracles

- **Primary:** multi-provider oracle aggregation (e.g., Chainlink/Pyth blend) with validity and staleness bounds.
- **Safeguards:** deviation limits per block, heartbeat limits, and failovers for oracle outages. The final oracle set will be determined prior to launch.

3.4 Liquidations & Funding

- **Funding:** premium between index price and mark price is continuously settled in batch intervals.
- **Liquidations:** triggered upon margin shortfalls; penalties are calibrated to prevent predatory liquidations while preserving market integrity.

3.5 Settlement Layer & Scaling

- The protocol deploys **critical integrity commitments** on Ethereum L1 to guarantee trustless settlement, while offloading batch execution and matching to a **distributed privacy-preserving settlement layer**. This ensures both high throughput and confidentiality of order flow.
- Future versions may explore alternative scaling layers while retaining the integrity model.

4. Token & Economics

4.1 Token Summary (per uploaded plan)

- **Ticker:** \$HEXA
- **Total supply:** 1,000,000,000
- **Burn at launch:** 930,000,000 (93%) → **circulating 70,000,000 (7%)**
- **Distribution of circulating:** LP ~50,000,000; Team 10,000,000 (4-yr vest); CEX reserve 10,000,000 (multisig)
- **LP pairing:** initially targeted at \$500k USDC. 10M market cap

4.2 Fair Launch & No Insider Deals

- **No KOL supply, no OTC allocations, no pre-mine favors.**
- **5% buy/30% sell tax at launch** to disincentivize snipers and protect long-term investors. 30% sell tax will gradually decrease over the first 24hrs post launch to 5%.
- **Tax ceiling hard-coded** for holder safety (can only be decreased).

4.3 Revenue Model & Holder Rewards

- **100% of protocol revenue** (e.g., trading fees, borrow/funding spreads, withdrawal fees if any) is paid out as ETH to token holders pro-rata by balance.
- **Operations financed solely** by the 5% buy/sell tax.

Mechanics (distribution):

- **Epochs:** Revenue accrues in **weekly** epochs.

- **Snapshot set:** balances snapshotted at fixed block intervals to minimize wash-trading games around distribution.
- **Direct ETH airdrop:** At epoch end, a distributor **sends ETH** to eligible wallets.
- **Exclusions:** Protocol contracts, burned addresses, and CEX wallets (unless the exchange opts in to per-user passthrough) are excluded or handled via formal whitelisting agreements.

4.4 Treasury, Tax & Budgeting

- **5% buy/sell tax** funds: Development, marketing, audits, salaries, bounties, infra, liquidity support, research, and grants.
-

5. Security & Trust

- **Audits:** external audits prior to MVP and major upgrades, as well as an audit of the smart contracts of the \$HEXA token.
 - **Bug bounties:** public program at MVP.
 - **Key management:** multisig for treasuries
 - **MEV mitigation:** Protect RPC and builders for order ingestion; batch auctions reduce sandwich and latency games.
 - **Resilience:** circuit breakers on oracle deviation; auction backstops for disorderly liquidations.
-

6. Go-To-Market & Ecosystem

- **Target users:** retail, funds/prop desks, market makers.
 - **Distribution channels:** Aggregator listings (e.g., routers, dashboards), analytics (Dune), research write-ups, and transparent performance reporting.
 - **Partnerships:** oracle providers, RPC/MEV-protect relays, custody and tax/reporting vendors (for funds).
-

7. Roadmap

Step 1. Laying the Foundation

This quarter is all about getting the basics right.

- We're running a **private test version** of the exchange, just with ETH and BTC, to make sure the hidden-order system (privacy feature) and batch trade matching works smoothly.
- We're putting in place the first version of our **safety system** that ensures traders can't take on more risk than they should.
- We're also setting up a **price feed system** so the exchange always knows the real market price of assets.

👉 In short: we're building the "engine room" of Hexa and testing it behind the scenes.

Step 2. Closed Beta → Open Beta

We'll start letting real users try Hexa.

- First, a **closed beta** (invite-only) so we can work closely with testers. Then we'll open it up for a **public beta on testnet**.

- Traders will get access to more advanced features like margin trading, partial liquidations (so you don't lose everything at once), and early funding mechanics.
- We'll also run the **first real ETH revenue airdrops** to HEXA holders so people can experience the reward system in action.
- Partner integrations with popular wallets and trading dashboards will start to roll out.

In short: users get their first hands-on experience with Hexa, and holders start seeing ETH flow to their wallets.

Step 3. Mainnet Launch

This is the official start of live trading.

- We'll launch on **mainnet** with ETH, BTC, and one more altcoin perpetual market.
- Traders will see privacy features expanded to cover **stop-loss and take-profit orders** as well.
- An **insurance fund** will be introduced to protect against extreme market events.
- Market makers (the traders who provide liquidity) will get special incentives, improving trading conditions for everyone.
- ETH airdrops continue weekly, and we'll start offering more flexible options for how holders receive them.

In short: Hexa goes live for everyone, with real money trading, real rewards, and a system built for stability and fairness.

Step 4. Project X

There is an additional (for now) secret “project x” in the works, which we think is going to alter the future of onchain trading forever. It is not a private perp DEX. More will be revealed in the coming months.

Clear timelines will be given once we are confident that we can meet them. We aim to underpromise and overdeliver and thus are taking a careful approach to giving clear dates/deadlines.

8. Token Utility & Holder Rights

- **Economic right:** pro-rata share of **all protocol revenue** as **ETH** (distribution policy adjustable by governance within guardrails).
 - **Governance right:** vote on key decisions (coming soon).
 - **No claim to equity or ownership** of any legal entity; the token conveys protocol-level rights only.
-

9. Risks & Mitigations

General Disclaimer

Hexa DEX is an experimental protocol in decentralized finance. The development of a **privacy-preserving perpetual futures exchange** has never been attempted at this scale before, and there are inherent uncertainties in both the technical design and the broader market environment. Nothing in this document constitutes investment advice, legal advice, or a guarantee of performance.

Key Risks

1. **Technical Risk**

- Smart contracts, cryptographic systems, and blockchain infrastructure may contain unknown bugs or vulnerabilities. Even with audits and bounties, exploits can occur and may lead to partial or total loss of funds.

2. Market Risk

- Trading in cryptocurrency derivatives is inherently volatile. Users may lose part or all of their funds due to leverage, rapid price movements, or unforeseen liquidity events.

3. Governance & Treasury Risk

- Treasury management relies on multisig signers. Malicious activity could affect treasury stability or protocol development.

4. Regulatory Risk

- Laws governing cryptocurrencies and decentralized exchanges vary across jurisdictions and may evolve rapidly. Access to Hexa may be restricted in certain regions, and regulatory changes could impact protocol operations or user eligibility.

Mitigations

- **Audits & Bounties:** All major contracts will undergo third-party audits, and a live bug bounty program will incentivize responsible disclosure of vulnerabilities.
- **Gradual Rollout:** Features will be released in stages (alpha → closed beta → open beta → mainnet MVP → full release) to limit exposure while we test and refine.
- **Resilient Design:** Redundant oracles, circuit breakers, and insurance funds will be implemented to reduce systemic risk.

- **Transparency:** All treasury wallets, burns, and revenue distributions will be published on-chain and openly auditable by the community.
- **Compliance Awareness:** We will consult legal experts while making clear that users are responsible for understanding and complying with their local regulations.
- **Clear Communication:** Users will be consistently reminded that trading is high-risk and that participation is voluntary, with no guarantees of profitability.

Final Statement

We cannot and do not guarantee the success of Hexa DEX or the preservation of user capital. What we can promise is our **utmost diligence, transparency, and commitment** to building the platform as securely and responsibly as possible. Participation in Hexa - whether as a trader or token holder - carries inherent risk.