

AlphaX Protocol: Trustless Performance — Technical White Paper V2.0 for the Next- Generation Hybrid Architecture Derivatives Trading Protocol

Trustless by Design. Performant by Engineering.

Abstract

As decentralized finance (DeFi) evolves toward institutional-scale adoption, the industry faces a fundamental technical contradiction: **on-chain transparency and trading performance cannot be achieved simultaneously**. Fully on-chain DEXs are constrained by the throughput of their underlying public blockchains, resulting in high latency, MEV attacks, and high gas costs. Centralized exchanges, while highly performant, expose users to unauditable counterparty risk through opaque asset custody.

AlphaX Protocol introduces an innovative **trustless performance architecture** that delivers the following through a decoupled three-layer design:

- **Sub-millisecond matching latency**, with peak throughput exceeding 100,000 TPS.
- **100% on-chain asset verifiability**.
- **Zero-KYC access**, with on-chain behavioral analysis to meet compliance requirements.
- **Unified multi-chain asset settlement**, with native support for four major networks: Ethereum, Arbitrum, BSC, and Tron.
- The contract architecture includes **forced withdrawal** capability to ensure traceable asset security.

1. Industry Pain Points and AlphaX Vision

1.1 The Industry Trilemma

The decentralized trading sector has long faced an "impossible trinity": **security, performance, and user experience** cannot all be achieved at once.

- **Security-first solutions** (e.g., fully on-chain AMM/order book DEXs): Assets are fully verifiable on-chain, but are limited by the TPS bottleneck of the underlying blockchain — resulting in high latency, expensive gas fees, and vulnerability to MEV sandwich attacks.
- **Performance-first solutions** (e.g., centralized exchanges): Offer ultra-fast matching, but the black-box custody model exposes users to systemic risks such as fund misuse and lack of auditability.
- **Compromise solutions** (e.g., appchains and ZK-Rollups): These seek a balance between security and performance, but each faces engineering challenges — including insufficient cold-start security for new chains, proof generation latency, and limited multi-chain compatibility.

1.2 AlphaX's Technical Approach

AlphaX has chosen a **pragmatic yet innovative** path — one that avoids building a new chain or relying on general-purpose proof systems that are not yet fully mature. Instead, it:

Achieves trust minimization through engineering innovation on existing, battle-tested blockchain networks.

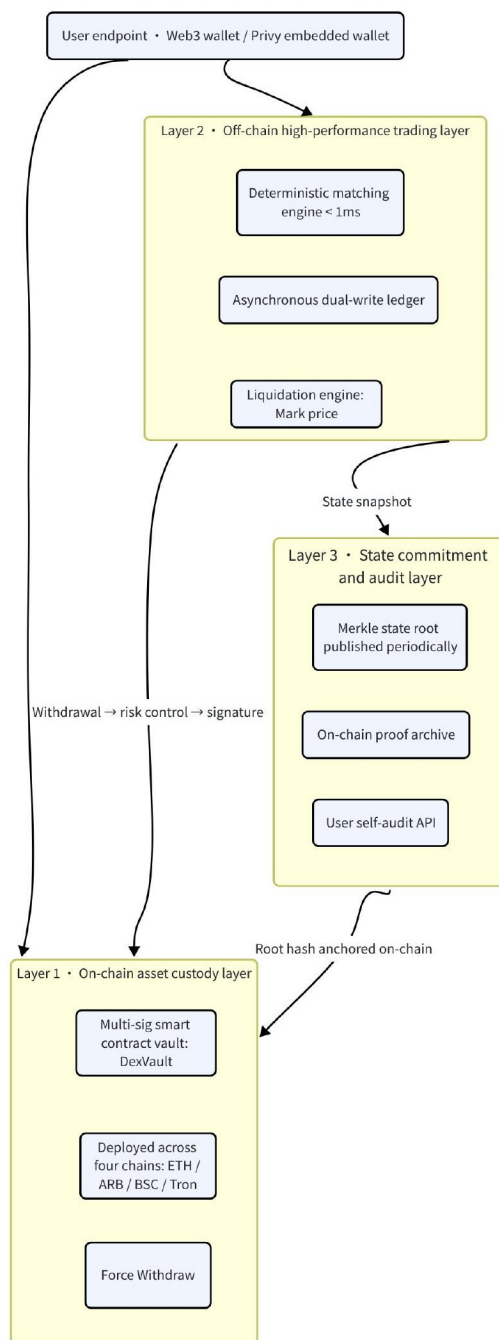
Core design principles:

1. **On-chain full custody** — asset security is protected by mature public blockchains such as Ethereum.
2. **Deterministic off-chain matching** — trading performance is ensured by dedicated computing clusters.
3. **Cryptographic state commitment** — transparency is guaranteed by mathematics.

2. Core Architecture

2.1 Three-Layer Decoupled Architecture

AlphaX's architectural philosophy: **"let each layer do what it does best"**:



Clear division of responsibilities across layers:

Layer	Core responsibilities	Trust model
On-chain custody layer	Asset custody and deposit/withdrawal execution	Protected by a multi-signature contract (on-chain auditable)
Off-chain trading layer	Order matching, position management, and risk control	Partial trust (auditable)
State commitment layer	On-chain verifiability of off-chain states	Cryptographic assurance

2.2 Design Decisions and Technical Trade-Offs

Why multi-chain native deployment instead of a custom L1?

- Inherit the security and decentralization of mature networks like Ethereum — no need to build a validator network from scratch.
- Users don't need to bridge assets to a new network, eliminating bridging risk and migration friction.
- **"Don't move users. Go to the chains users are on."** — Deploy independently security-audited smart contracts on each chain.

Why choose state commitments over ZK proofs?

- State commitments (Merkle root + inclusion proof) can be generated in seconds without proof-generation latency.
- Compatible with any blockchain, not limited to a single ecosystem.
- Engineering complexity stays manageable, while leaving room to integrate ZK-Coprocessor in the future.

3. On-Chain Custody Layer

3.1 Multi-Sig Vault Contracts

All user assets are held in **DexVault smart contracts**, independently audited by **BlockSec**. The contracts adopt a **UUPS architecture**, enabling secure and controlled upgrades. Meanwhile, withdrawals require **joint authorization from multiple independent signers (Multi-Sig)**, ensuring that the compromise of any single key will not result in asset loss.

Security audit reports (BlockSec):

- EVM contract audit:[blocksec-audit.pdf](#)
- Tron contract audit:[blocksec-tron-audit.pdf](#)

Contract system (fully open source):

- **DexVault** — Core asset vault managing ETH and ERC-20 deposits and withdrawals, with built-in multi-signature authorization and withdrawal limits.

Source code repositories:

- EVM contracts (Ethereum / Arbitrum / BSC):[AlphaX-Protocol-Contract](#)
- Tron contracts:[AlphaX-Protocol-Contract-Tron](#)

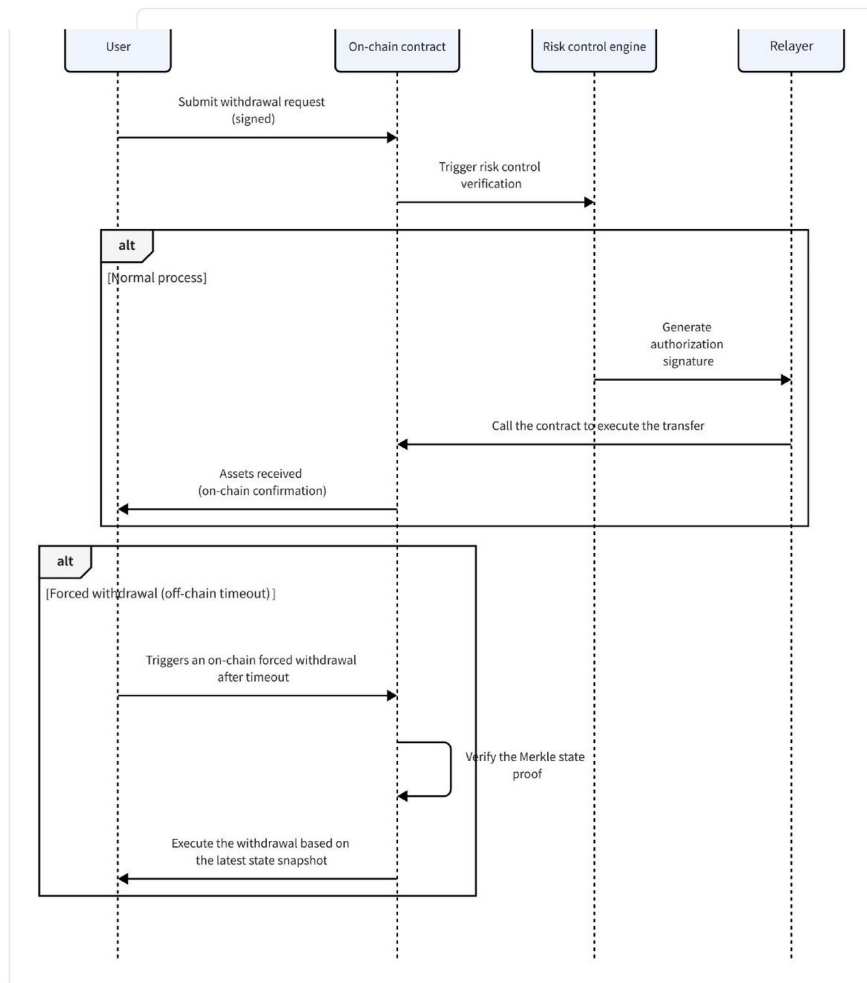


Key security mechanisms:

Mechanism	Implementation	Protection objective
Multi-sig withdrawals	Withdrawals require joint authorization from N-of-M independent signers	Eliminates single-key risk
On-chain withdrawal limits	Built-in per-token daily withdrawal limit enforced at the contract level	Caps losses even if signatures are compromised
KMS key custody	Signing keys are encrypted and stored in a hardware security module (HSM)	Keys never appear in plaintext throughout their lifecycle
Hot and cold wallet segregation	Large assets are held in cold wallets; hot wallets retain only what operations require	Reduces the online attack surface
Operator privilege separation	Withdrawal executors are separate from signing authorizers and contract administrators	Principle of least privilege

3.2 Forced Withdrawal

In extreme cases (such as platform downtime or an unresponsive relay), users can trigger a forced withdrawal directly through the on-chain contract, **without relying on any off-chain system**.

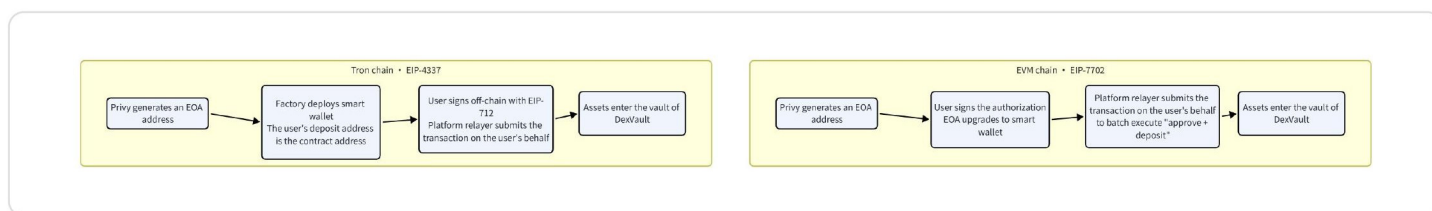


Key design features of this mechanism:

- **Per-user granularity** — One user's forced withdrawal does not affect other users' normal trading.
- **State proof-driven** — Executed based on the most recent on-chain anchored Merkle state root.
- **No off-chain dependency** — Even if all off-chain systems go down, users can still recover their assets independently.

3.3 Gasless Account Abstraction Deposit

Through account abstraction technology, AlphaX enables users to complete on-chain deposits **without holding any native tokens (ETH/BNB/TRX) for gas fees**, greatly lowering the barrier for Web2 users entering DeFi.



EVM chains (Ethereum / Arbitrum / BSC) — EIP-7702 solution:

EIP-7702 is a lightweight account abstraction standard introduced in Ethereum's Pectra upgrade. It seamlessly upgrades a regular EOA address to a smart contract wallet — no separate contract address management required.

- Once users generate an EOA address via Privy, they only need to sign the authority once to upgrade the address to a smart wallet.
- The platform relayer collects user signatures, then batches the "approve + deposit" operations into a single transaction and submits it on-chain.
- Supports gas-free deposits of **any ERC-20 token** on EVM chains.
- The contract uses a minimal feature set design (based on the OKX contract template), supporting only multicall and signature-verified multicall to minimize the attack surface.

Tron chain — EIP-4337 solution:

Since the Tron network does not yet support EIP-7702, AlphaX uses the EIP-4337 account abstraction solution to deploy a dedicated GasFree smart contract wallet for each user — no energy or bandwidth required.

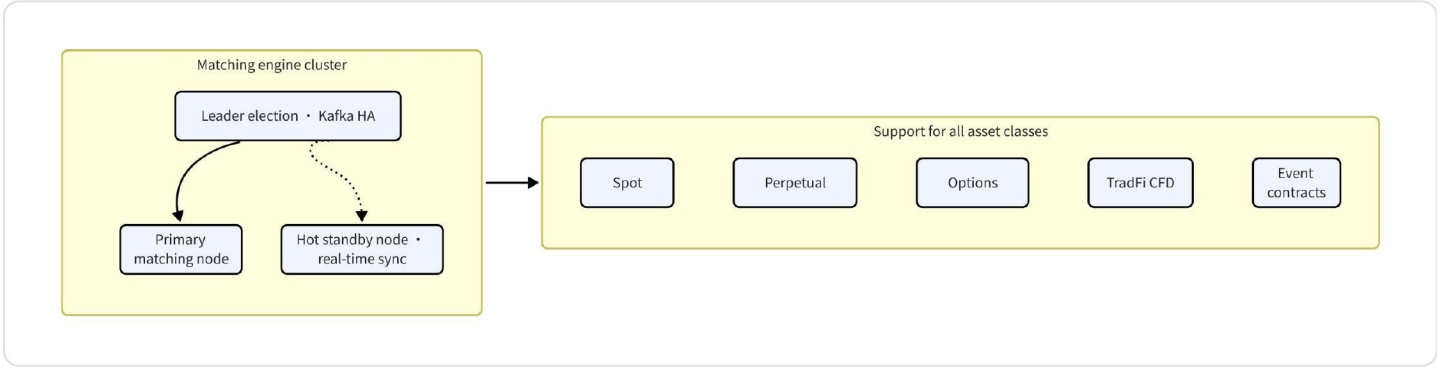
- **GasFreeFactory** — factory contract that batch-creates user smart contract wallets.
- **GasFreeAccount** — user asset management contract, with the user's EOA address as the owner.
- **GasFreeController** — relay contract handling EIP-712 signature verification and deposit logic.
- Based on Tron's official GasFree solution, users never need to hold TRX.

Consistent user experience: Regardless of chain or account abstraction solution, the experience is identical — sign up to get a deposit address, sign off-chain to complete the deposit, all with zero gas.

4. Off-Chain Execution Layer

4.1 Deterministic Matching Engine

The matching engine uses a **deterministic state machine** design. The same input always produces the same output, ensuring the matching process is replayable and auditable.

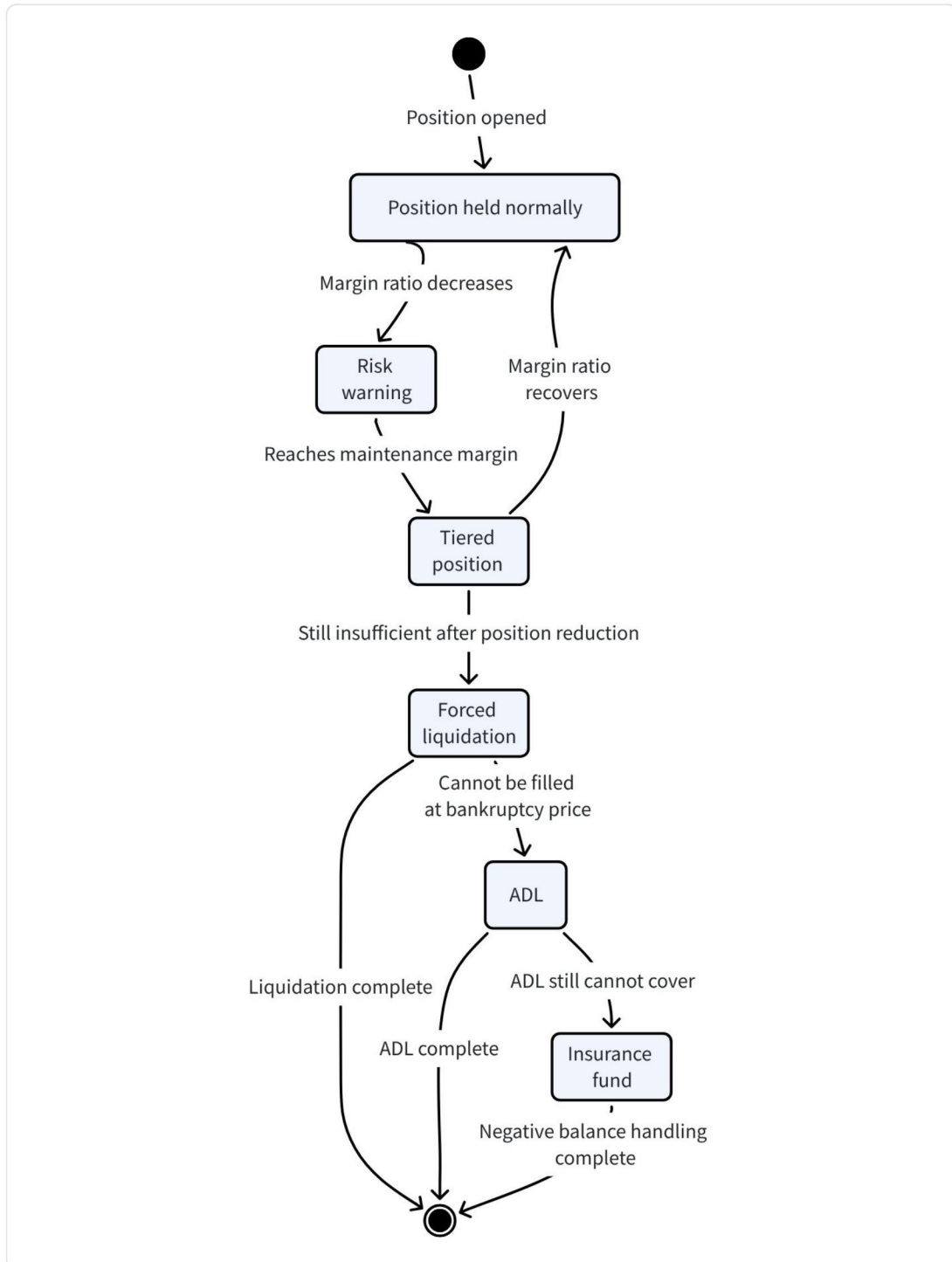


Performance metrics:

Metric	Value
Matching latency	< 1 ms (P99)
Peak throughput	> 100,000 TPS
Availability	99.99% (Leader election HA)
Order types	Limit / Market / Stop / IOC / FOK / Post-only

4.2 Multi-Level Liquidation System

AlphaX uses a tiered liquidation mechanism based on **mark price** to prevent unnecessary liquidations triggered by abnormal market conditions such as wicks:



Liquidation characteristics:

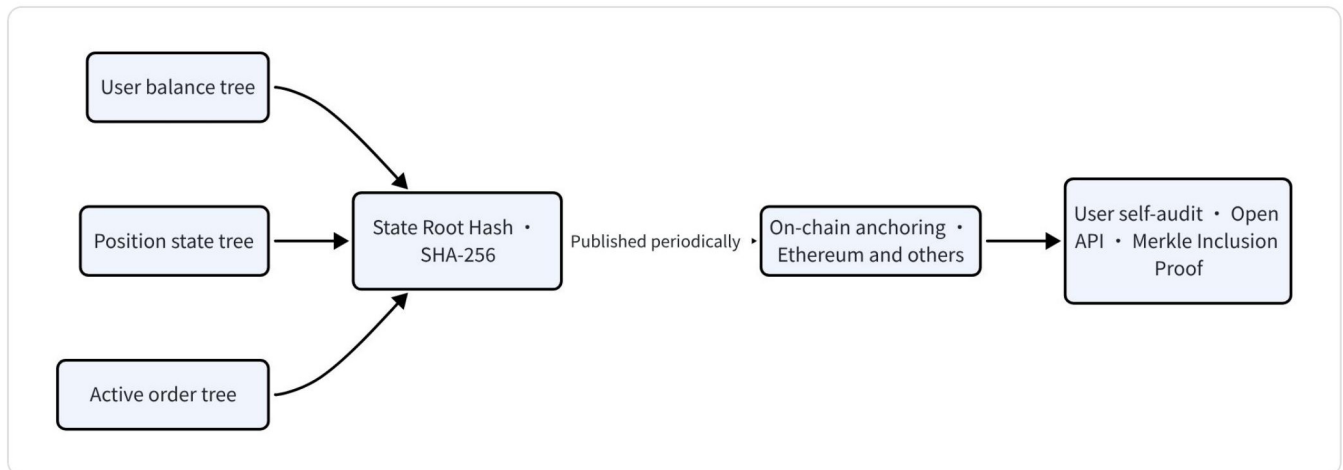
- **Tiered liquidation** — prioritizes partial position reduction to minimize impact on users.
- **Mark price liquidation** — uses a multi-source index price (VWAP/TWAP) to prevent malicious wick manipulation.
- **ADL** — in extreme conditions, automatically reduces winning positions by priority.
- **Insurance fund backstop** — the last line of defense against systemic risk.

5. Cryptographic State Commitment

This is a **fundamental trust upgrade** for AlphaX over traditional centralized exchanges.

5.1 Merkle State Tree and On-Chain Anchoring

All key off-chain states — user balances, positions, and active orders — are organized in a Merkle tree, with the root hash anchored on-chain periodically:



How it works:

1. The off-chain system calculates a global Merkle state root every N trade batches.
2. Submits the root hash and state delta data to an on-chain smart contract.
3. Any user can retrieve the Merkle inclusion proof for their account via the open audit API.
4. Users can independently verify that their assets are included in the global state.

5.2 Proof of Reserves

AlphaX publishes periodic Proof of Reserves, letting users verify the platform's solvency without trusting any third party:

1. **Total on-chain assets** — anyone can check vault contract balances via a blockchain explorer.
2. **Off-chain liability proof** — publishes the aggregate root of all user balances via a Merkle sum tree.
3. **1:1 solvency verification** — on-chain assets $\geq$ the Merkle sum root of off-chain liabilities.

6. Dual-Track Account System

6.1 Zero-Barrier Access

AlphaX has built a privacy-focused, KYC-free account framework that serves both Web3-native users and new Web2 users:

Web3-native path:

- Supports EIP-712 signature verification with mainstream wallets including MetaMask and OKX Wallet.
- Users retain full control of their private keys — the platform stores no key fragments.
- On-chain address as identity (address-as-identity)

Web2-friendly path:

- One-click sign-up via Email, Google, and other social channels.
- Privy automatically generates an embedded wallet in the background, with private keys stored via TSS sharding.
- The platform cannot access the full private key independently, and users can export it to an external wallet at any time.

6.2 Compliant On-Chain Behavior

Following Web3's privacy-first principle, AlphaX shifts the core functions of compliance and anti-money laundering (AML) away from traditional identity-based approaches:

- **On-chain behavioral analysis** — driven by transaction pattern recognition, not identity verification.
- **Geofencing** — precise access controls powered by intelligent IP-based routing.
- **LiteFlow dynamic rules engine** — hot-reloading risk control rules with visual orchestration, effective within 10 seconds.

7. Full-Spectrum Trading

AlphaX is more than a derivatives trading protocol — it is a **unified trading infrastructure for all asset classes**:

Crypto assets: Spot · Perpetual futures · Options · Margin trading

Traditional financial assets: Gold / Silver (XAU/XAG) · Forex (EUR/USD · GBP/USD) · Stock indices (US30 · SPX)

Innovative categories: Event contracts / Predictions (CeDeFi model) · Bots (Grid / Martingale) · Copy trading

All categories share a unified margin account, liquidation engine, and risk control matrix — enabling users to trade all asset classes from a single account.

8. Comprehensive Security Architecture

8.1 Five Layers of Defense in Depth

AlphaX has built five layers of security depth spanning on-chain and off-chain systems:

Layer 1 · On-chain contract security

- UUPS upgradeable contracts (upgrade permissions governed by multi-sig) · Independent security audit by BlockSec · Open-source contract code

Layer 2 · Trading engine security

- Deterministic matching (replay-verifiable) · Memory-safe isolation · Leader election HA (99.99%)

Layer 3 · Risk control engine

- LiteFlow dynamic rules (hot reloading) · Multidimensional behavior analysis · Tiered liquidation + ADL

Layer 4 · Withdrawal security

- Idempotency and replay protection · Deadline validation · Hot and cold wallet separation · Large-amount cold wallet routing

Layer 5 · Asset verifiability

- Merkle state proof (anchored on-chain) · Proof of Reserves (PoR) · forced withdrawals (per-user granularity)

8.2 Institutional-Grade Liquidity Assurance

- **Global professional market maker network** — 24/7 two-way quotes to prevent liquidity gaps during extreme market conditions.
- **Ultra-tight bid-ask spreads** — Provides deep, tight multi-level liquidity for major assets, reducing the market impact of large market orders.
- **Fair price anchoring** — Quotes derived from aggregated multi-source market data (VWAP/TWAP), with independent monitoring sentinels detecting abnormal deviations in real time.
- **Circuit breaker protection** — Automatically triggered when prices deviate abnormally, protecting users from manipulation.

9. Conclusion

AlphaX Protocol has chosen a practical yet ambitious path: achieving trust minimization through engineering innovation on existing, well-proven blockchain networks:

- **Practical** — Built on mature networks such as Ethereum, Arbitrum, BSC, and Tron as the asset security layer, inheriting their security protections.
- **Ambitious** — Push transparency to a DEX-level standard through cryptographic state commitments, forced withdrawals, and Proof of Reserves.
- **Open** — The ultimate goal is to become an open protocol enabling frictionless participation across all asset classes, the omnichain ecosystem, and all trader types.

AlphaX's ultimate vision is to become the **trustless infrastructure layer for global asset trading**.

AlphaX Protocol — Where Trust Meets Performance.