Universal Perps Protocol: A Technical Whitepaper

October 12, 2025

Table of Contents:

---

1. Abstract

The Universal Perps Protocol is a next-generation decentralized exchange for perpetual futures, engineered for CEX-like performance, permissionless access, and verifiable, non-custodial security. It introduces a high-performance hybrid architecture that combines an **off-chain trading engine** for gas-free, real-time trade execution with an **on-chain settlement layer** for decentralized custody and trustless verification.

This model fundamentally addresses the asset onboarding limitations and high transaction costs of existing protocols by enabling the instantaneous, gas-free creation of perpetual markets for any on-chain token. The protocol's core logic—a fully synthetic engine, a Proactive Leverage Protocol (PLP), and a Dynamic Funding Rate—runs on the high-speed off-chain engine.

Protocol security and decentralization are guaranteed by the on-chain `CollateralVault` smart contract, which holds 100% of user collateral non-custodially. The off-chain engine periodically commits a cryptographic "state root" to the blockchain, allowing any user to verify the system's solvency and execute "forced withdrawals" directly from the smart contract, ensuring the protocol remains trustless.

2. Introduction: The Limitations of Current Perpetual DEXs

Decentralized perpetuals protocols have emerged as a cornerstone of DeFi, yet their growth is constrained by key architectural challenges:

- **Permissioned Asset Onboarding:** The creation of new markets is typically a slow, governance-gated process, preventing traders from capitalizing on nascent or long-tail assets.
- **High Gas Costs & Latency:** Purely on-chain protocols require users to pay gas for every action (opening, closing, modifying leverage), creating a slow and expensive user experience that cannot compete with centralized exchanges.
- **Capital Inefficiency:** Many models rely on dedicated liquidity pools (LPs) for each asset, fragmenting capital and creating dependencies on LP incentives, which leads to shallow market depth.
- **Reactive Risk Management:** Protocols often rely on reactive mechanisms like socialized losses or complex auto-deleveraging (ADL) systems, which penalize successful traders and erode user trust.

Universal Perps Protocol is designed from the ground up to solve these core issues, offering a permissionless, capital-efficient, and gas-free trading experience built on a foundation of decentralized, verifiable settlement.

3. Core Architecture: A High-Performance Hybrid Model

The protocol's foundation is a hybrid system that separates the "fast" trading logic from the "slow" custody and settlement, providing the best of both centralized and decentralized worlds.

3.1. The Off-Chain Trading Engine (The "Fast" Layer)

The core trading experience is managed by a high-performance centralized server, enabling gas-free, real-time operations. This engine is responsible for:

- **User Authentication:** Users connect their wallet and sign a gas-free message to authenticate with the trading engine, linking their on-chain address to a secure, off-chain account.
- **Gas-Free Trading:** All trading actions—opening positions, closing positions, and setting leverage—are gas-free API requests processed instantly by the engine and recorded in a high-speed database.
- **Synthetic Engine & PnL:** The engine operates as a sophisticated "paper" accounting ledger, creating virtual long and short contracts between participants. It does not trade spot assets, allowing for the creation of markets on any token. It calculates all user PnL in real-time.
- **Core Logic Execution:** All complex calculations, including the Proactive Leverage Protocol (PLP) and Dynamic Funding Rates, are executed by this server, imposing no gas cost or on-chain burden.

3.2. The On-Chain Vault & Settlement Layer (The "Trust" Layer)

The protocol's security and non-custodial guarantee are enforced by a set of audited smart contracts. This is the "trust" layer where all user funds are secured.

- **`CollateralVault.sol`:** This is the protocol's core smart contract. It holds 100% of all user collateral (denominated in a primary stablecoin, e.g., USDC). This contract is the only component users must trust with their funds. All user deposits and withdrawals are processed through this non-custodial vault.
- **`Staking.sol`:** A standard staking contract that allows UPX token holders to stake their tokens and receive their pro-rata share of protocol revenue.

3.3. Trustless Verification: State Commitments & Oracles

To ensure the off-chain engine is honest and solvent, its state is cryptographically bound to the on-chain vault.

- **Off-Chain State Commitments:** At regular intervals, the off-chain engine calculates a **Merkle Root**—a single cryptographic hash that represents the entire state of all user balances in its ledger. The engine then posts this "state root" to the `CollateralVault` smart contract in a single, cheap on-chain transaction.
- **On-Chain Forced Withdrawals:** This mechanism empowers users and makes the protocol trustless. To withdraw, a user requests a "Merkle Proof" from the server. They can then present this proof to the `CollateralVault` contract. The contract can verify on-chain that the user's proof is valid for the latest state root and that they are entitled to their funds. This ensures that users can always withdraw their funds, even if the off-chain server is offline or malicious.
- **On-Chain Liquidation Oracle:** While the off-chain engine uses various price feeds for PnL calculation, all *liquidations* are verified against a secure, on-chain oracle (e.g., Chainlink or a TWAP). This prevents the server from triggering malicious or unfair liquidations, as any liquidation must be proven valid against the on-chain "source of truth."

4. The Dual-Pillar Stability Model

The protocol's solvency is managed by two symbiotic mechanisms that run on the **off-chain engine**.

4.1. Proactive Leverage Protocol (PLP)

The PLP is the protocol's primary defense, preventing systemic risk before it can be created. This logic is executed by the off-chain engine before any gas-free trade is accepted. It analyzes the trade's impact on the market's net open interest (OI) imbalance.

The protocol algorithmically splits every trade into two components:

1. **Matched Portion:** The portion of a trade that reduces the market's OI imbalance. This portion is considered balanced and is eligible for maximum leverage (e.g., up to 100x).
2. **Unmatched Portion:** The portion of a trade that *increases* the market's OI imbalance. This portion is considered an unsecured bet against the entire collateral pool and is **restricted to 1x leverage only**.

This non-negotiable rule makes it impossible for any actor to build a large, leveraged position that could threaten protocol solvency.

4.2. Dynamic Funding Rate Mechanism

While the PLP acts as a gatekeeper, the Dynamic Funding Rate acts as a continuous economic pressure system. This rate is calculated by the off-chain engine and settled as a balance update in the off-chain ledger. The funding rate is a direct function of the OI skew.

- **Mechanism:** The dominant side of the market (e.g., longs) pays a periodic funding fee to the minority side (e.g., shorts). The magnitude of this fee is proportional to the degree of imbalance.
- **Dual Function:**
    1. **Disincentivization:** It imposes a significant, ongoing cost on traders who maintain large, unbalancing positions.
    2. **Incentivization:** It creates a highly profitable arbitrage opportunity, attracting traders to take the minority side and naturally drive the market back towards equilibrium.

5. Protocol Economics & Fee Structure

The protocol is designed as a sustainable business, generating revenue exclusively from user activity.

5.1. Revenue Streams

1. **Trading Fees:** A flat fee of 0.1% is applied to the notional size of every trade (both opening and closing).
2. **Liquidation Fees:** A minor penalty fee is assessed on the remaining collateral of liquidated positions.

5.2. Fee Allocation Model

All generated fees are programmatically allocated to ensure the long-term health and decentralization of the ecosystem:

- **25% to the Insurance Fund:** This fund is the protocol's first line of defense to cover any potential bad debt arising from extreme market volatility where a liquidated position's collateral is insufficient.

- **37.5% to UPX Token Stakers:** This portion is distributed as a real-yield revenue share to users who stake the native UPX token, aligning their interests with the protocol's success.
- **37.5% to Core Development:** These funds are allocated to the ongoing development, maintenance, and operational costs of the protocol and the off-chain engine.

6. The UPX Token & Utility

UPX is the native governance and utility token of the Universal Perps Protocol.

6.1. Governance

UPX token holders will have the power to govern the protocol via a Decentralized Autonomous Organization (DAO). Voting rights will extend to key on-chain decisions, including:

- Adjusting protocol parameters (e.g., trading fees, funding rate coefficients).
- Approving expenditures for ecosystem growth.
- Managing upgrades to the protocol's smart contracts.

6.2. Revenue Share

By staking UPX tokens, holders are entitled to a pro-rata share of 37.5% of the protocol's trading fee revenue, creating a direct incentive to hold and participate in the ecosystem's success.

7. Governance Model

The protocol will launch under the stewardship of the core development team with a clear and committed path towards progressive decentralization. Upon maturation of the protocol and distribution of the UPX token, control of the on-chain contracts and key parameters will be fully transferred to the DAO, making Universal Perps a public good governed by its community.

8. Disclaimer

This document is for informational purposes only and does not constitute an offer to sell, a solicitation of an offer to buy, or a recommendation for any security or financial instrument. Trading derivatives and cryptocurrencies involves substantial risk and is not suitable for every investor. All trading strategies are used at your own risk. Please conduct your own thorough research before participating in the protocol.