Collateral Risk Analysis - Tokenized HLP

Anthias Labs

23 June 2025

Abstract

This report provides a comprehensive risk assessment of the Hyperliquidity Provider (HLP) vault and its tokenization mechanisms. HLP represents a novel approach to democratize market making and liquidation services, allowing community participants to collectively earn profits from activities traditionally reserved for institutional trading firms.

We identify and detail various risk types which are inherent in the HLP Vault. The analysis shows that while routine market-making risks remain well-managed, tail-event risks including coordinated manipulation attacks pose threats to vault stability. Historical validator interventions, while protective of HLP capital, introduce governance centralization concerns that may impact long-term credibility.

For tokenized HLP implementations, we examine two popular approaches: CoreWriter-based on-chain tokenization and manually-operated EOA methods. The report identifies depeg risks stemming from smart contract vulnerabilities, private key compromise, and market-driven selloffs as primary concerns for tokenized derivatives.

1 HLP Vault Overview

HLP is a community-owned vault on Hyperliquid's Layer-1 that serves as the primary market-maker and liquidation backstop for the exchange. Initially this included two vaults, a Market-Making vault which placed buy/sell orders to tighten spreads and a dedicated Liquidator vault for handling liquidations. In August 2023, the team merged the Liquidator into HLP for efficiency, so now HLP encompasses both continuous market-making and on-chain liquidation roles.

1.1 User Interaction and workflow

HLP generates returns through:

a) **Market Making:** Providing liquidity on Hyperliquid's order book, earning bid-ask spreads.

b) **Liquidations:** Managing overleveraged position liquidations, profiting from bonuses.

c) **Fee Accrual:** Earning a portion of trading fees (20% since Aug 2023).

d) **Funding Rates:** Gaining or paying funding based on net positions in perpetual contracts.

Users deposit USDC into HLP, receiving a proportional share of the vault. For example, a 100 USDC deposit into a 900 USDC vault grants 10% ownership. If the vault grows to 2,000 USDC without any other deposits, the user can withdraw 200 USDC, minus slippage. The share is proportionately reduced when new users deposit USDC in the vault.

A 4-day lock-up applies after any deposit, funds can only be withdrawn 4 days later to prevent rapid in-and-out arbitrage of short-term PnL. The vault charges no management or performance fees, unlike user-run vaults that take 10% of profits.

1.2 Strategy and Working

1.2.1 HyperCore Market Making

HLP's trading strategy is run off-chain by Hyperliquid team's algorithms, but it executes fully on-chain via HyperCore's orderbook. The strategy continuously calculates a fair price for each asset using a blend of Hyperliquid's own orderbook data and external market data for CEXes like Binance, Coinbase, BitGet etc. HLP's algorithms read live price feeds from these exchanges and the on-chain orderbook to estimate a robust fair value.

Around this, HLP places limit orders on both sides aiming to earn the bid/ask spread and sometimes takes trades to manage inventory or respond to momentum. This means HLP is not a passive LP; it actively adjusts orders, tightens spreads, and even takes advantageous orders to lock in profits or cut losses, behaving similarly to a high-frequency market maker.

1.2.2 Liquidation Mechanics

When a leveraged trader's position on Hyperliquid is about to go under margin, HLP acts as the liquidator. The system force-closes the position automatically if it goes below the margin threshold. HLP will take over that position, essentially buying it if the trader was long (or selling if the trader was short) and then immediately attempt to offload it on the orderbook or net it against its other positions.

By doing so, HLP earns a liquidation fee and prevents bad debt on the exchange. However, this exposes HLP to the risk that it may not exit the liquidated position at a favorable price (especially in a fast-moving or illiquid market).

1.3 Validator Overrides & Governance

One important aspect of Hyperliquid is that the validators can intervene in certain situations for risk mitigation. This came to light during the "JELLY incident" in March 2025: a manipulatively engineered short squeeze on a low-cap token (JELLY) led to HLP holding an unrealized loss of over $10M as the price spiked. Fearing that a small-cap could wipe out the $230M vault entirely, the team took an emergency action: they delisted the JELLY market and forced a settlement at a specific price (0.0095 USD), notably, the price where the attacker had opened their short.

In effect, they bailed out HLP by overriding the market and resetting that trade. This was done through the validator governance mechanism (essentially, the validators agreed to halt trading on JELLY and settle it at a chosen price). The move was controversial, since it overrode normal market forces to protect HLP's capital. In response, Hyperliquid introduced on-chain validator voting for delisting decisions going forward, aiming to add more transparency and decentralization to any such emergency interventions.

2 HLP's Historical Analysis

Over its full lifetime, HLP's track record can be characterized as positive with a consistently favorable risk/reward profile, affected by a few stress events.

2.1 Profit Making Strategy

HLP's returns have come from four primary sources:

- Market-making
- Funding rate accrual
- Trading fee revenue
- Closing over-leveraged positions

In H2 2023, trading on Hyperliquid was free, so HLP's profits then were purely from market making and funding. Starting June 13, 2023, Hyperliquid introduced fees (0.025%/0.002%)

which accrued entirely to HLP for a period. This gave HLP a steady income stream. In August 2023, Hyperliquid team adjusted the fee allocation: 20% of net trading fees go to HLP, with 40% to insurance assistance fund and 40% to trader rewards. Even after this change, HLP continued to earn substantial fees, but it reduced HLP's APR relative to early 2023. Counterbalancing that, in August 2023 HLP also took over the Liquidator role, meaning it started to earn liquidation fees and extra profits from handling liquidations (or losses, if a liquidated position is hard to exit).

The profit of HLP vault is equal to net loss of all traders combined.

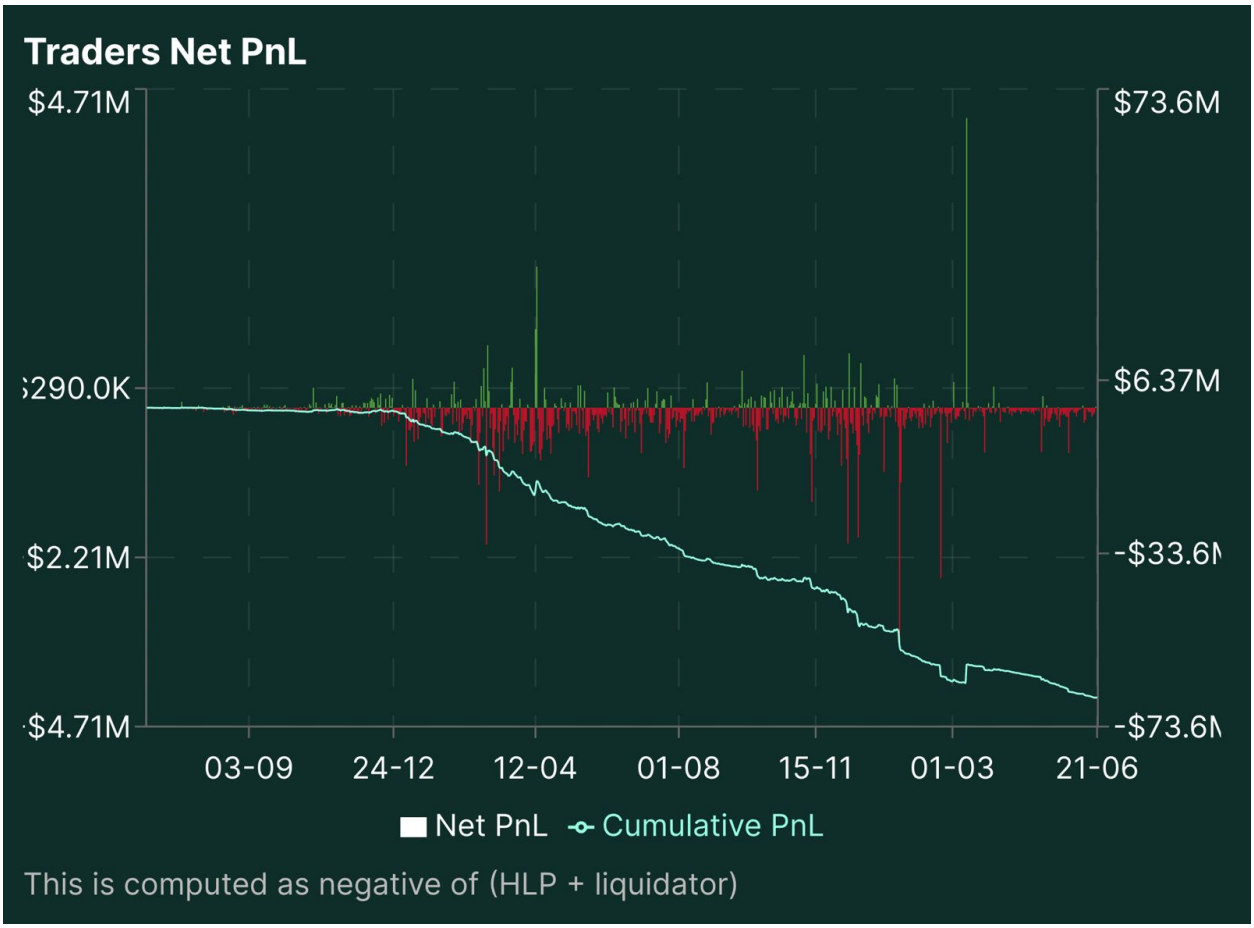

Figure 1: Source: Stats

2.2 Cumulative Returns

Right from the start HLP has yielded a high cumulative return for depositors. By the end of 2024 (roughly ˜19 months since launch), HLP had about $50 million in profit distributed to vault depositors. The vault's TVL at that time was around $350M, so if we compare profit to TVL as a rough measure, that's equivalent to ˜14% of the vault size earned as profit. However, many users deposited gradually over 2023, so early participants saw much larger proportional gains (since the $50M was earned on a smaller base for most of the time).

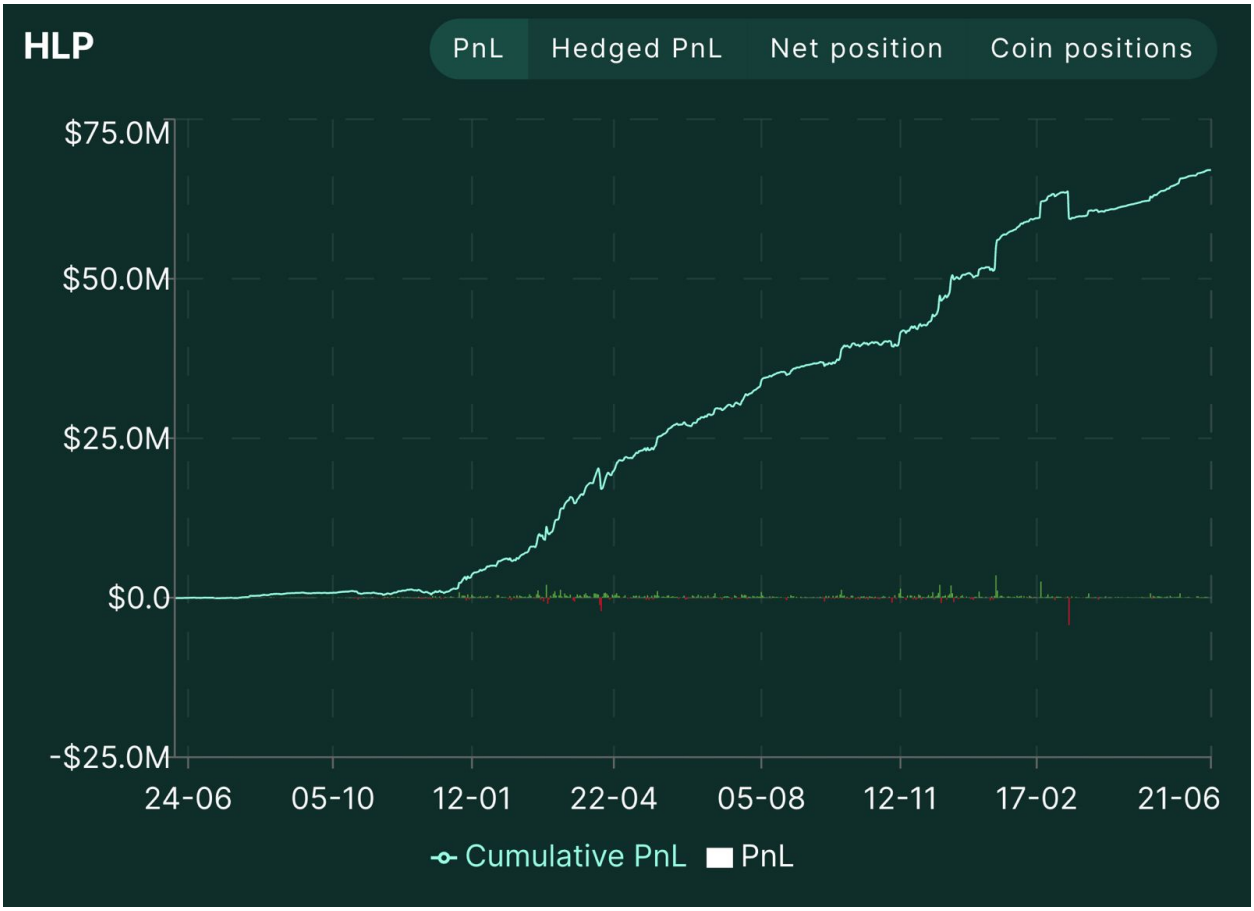

Figure 2: Net PnL of HLP | Source: Stats

2.3 PnL Over Time

One characteristic of HLP's performance is its consistency. The vault had continuous overall profitable months from launch through early 2025—there were losing days and a few losing weeks, but on a monthly basis, drawdowns were typically recovered quickly. In the first 15 months (mid-2023 through 2024), HLP's weekly returns were positive ˜90% of the time.

There were a handful of down weeks (six in 2024), but none of those exceeded a ˜1% loss until 2025's larger drop. The largest historical drawdown prior to 2025 was on the order of just ˜2–3%, which is remarkably low. The maximum drawdown on record came with the JELLY incident, where HLP faced a $4.28M loss. This in turn sparked a chain of withdrawals from the vault, reducing the TVL from $509M to ˜$150M. HLP took almost 2 months to cover this $4M loss.

Figure 3: HLP monthly returns | Source: Looping Documentation

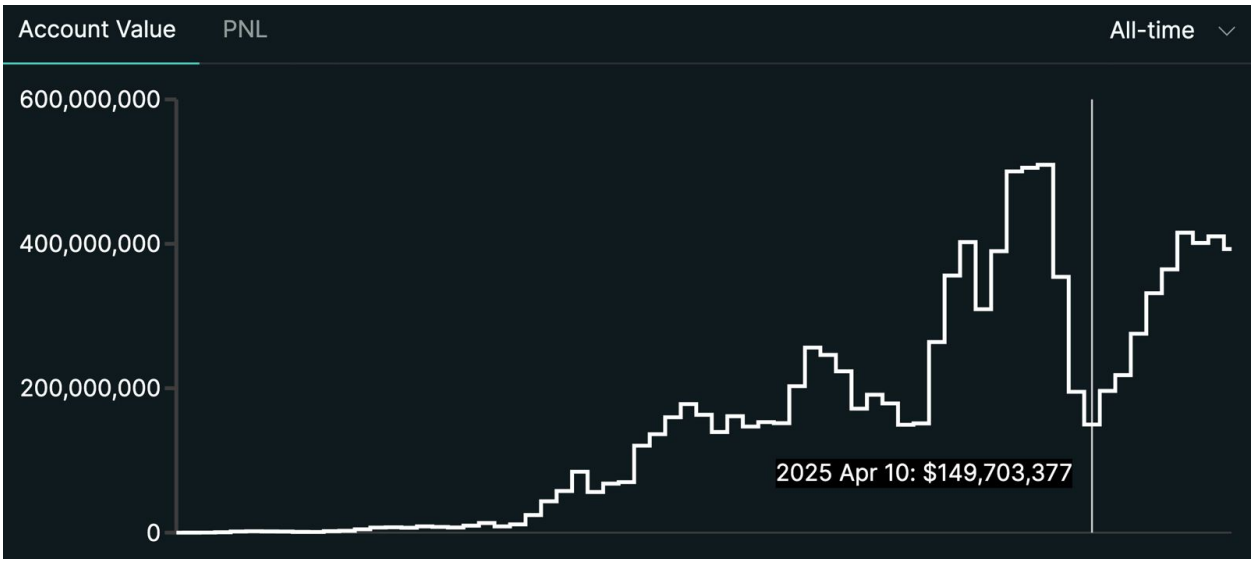

Figure 4: HLP Vault TVL | Source: Hyperliquid Dapp

3 HLP Native Risks

HLP's unique design brings in a variety of risks. Below we define the key risks, ranging from routine market risks to tail-event and structural risks.

3.1 Market-Making Risk

HLP profits by market-making, which inherently faces P&L volatility across markets. In calm or mean-reverting markets, HLP's strategy of providing liquidity and capturing spreads tends to make steady profits. In trending markets, HLP can be found leaning the wrong way e.g. net short in a persistently rising market or net long in a falling market leading to adverse P&L. This occurred notably in early 2023's bull run: traders were heavily long, HLP was net short and thus the raw PnL graph went down for that period. Such market-based losses are likely over a period as markets won't always favor HLP's style.

The severity is moderate: HLP's risk engine and active management keep losses bounded. For example, across 64 weeks in 2024-25, only 6 were negative, and none of those weekly losses exceeded a fraction of a percent until 2025's special events. The strategy adapts by widening spreads or reducing size in trends, and it benefits from funding payments in one-sided markets to offset directional losses. Overall, market-making P&L variance is a continuous risk but one that HLP has managed with Sharpe > 3 historically.

3.2 Whale Exploitation & Abuse Patterns

Because HLP is effectively the counterparty for trades, sophisticated whales might target HLP's weaknesses.

Self-liquidation schemes: a whale opens an enormous position knowing they can move the price against themselves to force a liquidation that HLP must absorb. The JELLY incident falls into this case. HLP was stuck with a massively underwater long position and an unrealized loss >$10M.

Oracle manipulation or spoofing: since validators post price oracles, a malicious actor could attempt to influence those or exploit any latency. If an oracle price is manipulated even briefly, a whale might enter trades at favorable prices or trigger force liquidations.

Such attacks are not regular, but a couple of these have already been seen in one year, hence medium likelihood. Attackers are incentivized by the large TVL (as HLP grew to hundreds of millions).

Severity of such attacks is **High**. The JELLY attack threatened HLP to lose everything to a low market cap memecoin in a $230M vault. Ultimately the team intervention limited the damage. But without the intervention, HLP could have lost a double-digit percentage of its assets in that single incident. Similarly, the $4M margin design exploit triggered a decrease in the maximum allowed leverage for multiple majors like BTC and ETH on the platform.

These attacks are easily detectable as whales are observable via on-chain footprints, e.g. one address accumulating huge positions or OI on an illiquid asset. In JELLY, the buildup was noticed, but not the intent until the squeeze happened. Hyperliquid now monitors OI spikes and has dynamic OI caps and loss thresholds to catch these in real-time. The introduction of validator voting for delisting also means if an asset's moves look fishy, validators can quickly halt it (as they did with MYRO in March 2025 due to manipulation risk). Despite these precautions, an attacker with enough capital could still attempt a coordinated multi-asset manipulation.

3.3 Oracle Drift / Validator Failure

Hyperliquid relies on validator-run oracles and regular price updates. If the oracle price drifts away from the actual price (say validators lag or fail to update during a fast move), the mark price used for liquidations could be off, leading to improper liquidations or trades. A validator outage or chain halt could freeze price feeds. This risk is inherent in any semi-centralized oracle system.

So far, Hyperliquid's oracles have operated smoothly. It would likely take a collusion or major bug for a significant drift to occur, which is considered low probability (the validator

set is small and known, so outright fraud is unlikely, and technical failure affecting all validators simultaneously is also rare).

Severity is high in this scenario. If, for example, the oracle froze while the real market moved 20%, traders could exploit stale prices to trade against HLP (HLP might still be quoting based on old mark). HLP could incur large losses or be stuck holding positions that are far off-market.

Detectability of this is somewhat low before it causes damage, because by the time system realises the oracle is wrong, trades may have happened. However, any significant oracle deviation would be quickly evident by comparing Hyperliquid's index to external market prices, something both users and the team would notice. The docs explicitly warn that if an oracle is compromised or manipulated for an extended time, "liquidations could occur before price reverts to fair value".

3.4 Governance Centralization & Emergency Interventions

Hyperliquid has demonstrated that in crises, the team/validators will intervene and override normal operations, effectively prioritizing HLP's solvency over strict decentralization. If HLP faces ruin due to some market event, one might expect another intervention (e.g., halting a market, manual deleveraging).

Such interventions won't happen daily, only in extreme scenarios, but given one already occurred within a year of launch, it's not far-fetched another could. The existence of on-chain voting now might slow down rash actions, but note that in the MYRO delisting, validators swiftly voted 4–0 to remove it due to manipulation risk, showing they are willing to act preemptively.

This one has two sides. Financially, interventions aim to reduce severity of losses e.g. saving HLP in case of $JELLY by capping the loss. So from a pure vault-value perspective, interventions limit the damage. However, the side-effects can be severe in other ways: they might hurt other users, and this definitely affects the perceived trust/decentralization. If such bailouts happen regularly, traders may fear any winning position could be nullified if it hurts HLP, damaging Hyperliquid's reputation.

These interventions are public (delistings announced, votes recorded). There is no private way to perform these operations, everyone knew JELLY was halted and why. So the risk here is not about hidden issues, but about governance decisions: it introduces governance risk that rules can change in edge cases. The detectability of centralization risk is high in the sense that users can gauge how many validators are team-controlled, and see how they vote. The trend so far: validators acted to protect the system.

3.5 Withdrawal Run & Liquidity Crunch

Similar to a bank run, if HLP suffers a drawdown or users lose confidence (e.g. after a big loss or exploit), many depositors might rush to withdraw their USDC once their lock-up expires. This happened in March 2025 and led to a 70% TVL drop in a few days, as shown earlier.

Likelihood for such a scenario is medium as it requires a trigger (major loss or fear event), but as we saw, such triggers did occur and could again. The lock-up delays withdrawals by 4

days, which slows a stampede but doesn't stop it – it just creates a queue. If multiple users have passed their lock, they can withdraw immediately. If many exit, the vault shrinks.

Such a run doesn't directly steal funds from HLP (unlike a bank, HLP is always fully collateralized by USDC and open positions). However, rapid outflows shrink HLP's capital, which can cause a liquidity crunch in two ways:

- HLP might have to scale down its market-making abruptly. If 40% of funds leave, HLP should ideally reduce its open positions by 40% to maintain similar leverage. It might need to widen spreads or withdraw some quotes, temporarily hurting exchange liquidity.
- If there's a queue of withdrawals, remaining depositors might get stuck with a larger share of further likely losses. For example, imagine a huge loss hits HLP, and some savvy users withdraw right before the losses fully materialize. The remaining user's capital bears the subsequent loss on open positions.

The liquidity crunch aspect also matters: if HLP becomes too small (TVL drops massively), it might not be able to effectively cover large trades on the exchange, and its PnL generation would also slow (less capital to deploy). There's also systemic liquidity risk if, for instance, a lot of USDC leaves Hyperliquid.

3.6 Smart-Contract or Chain-Level Exploits

Technical risks include bugs in the HLP contracts, flaws in HyperCore's L1 code, or exploits of the USDC bridge. Although Hyperliquid has been audited and runs a bug bounty, with no hacks so far. A contract vulnerability or bridge failure could let attackers drain or freeze funds, depeg or lock USDC, or miscalculate user balances.

Likelihood for such an attack is low as there is no specific evidence of vulnerabilities and the contracts were thoroughly audited. Severity of this case is extremely high. A hack or exploit could mean immediate loss of user funds.

4 Tokenization Methods & Related Risks

HLP can be tokenized via various mechanisms, each carrying distinct risk profiles and operational characteristics. Currently, two primary tokenization methods are being deployed on Hyperliquid.

4.1 Tokenization Mechanisms

4.1.1 CoreWriter-Based Tokenization

The upcoming CoreWriter contract offers a fully on-chain way to tokenize HLP. Users deposit funds directly from HyperEVM using the CoreWriter and it passes the funds through to the HLP vault on HyperCore. Redemptions work in reverse order, CoreWriter is used to withdraw funds using the corresponding vault share, and USDC is sent back to the redeemer.

Because deposits, withdrawals, and accounting are all done using smart contracts and settled atomically, this path is the most decentralized and transparent.

4.1.2 Manually-Operated Tokenization

Projects are currently launching tokenized HLP through manual deposits into the HLP vault using an EOA (Externally Owned Account) cold wallet after collecting user funds. This method serves as the only available option on mainnet until CoreWriter goes live. The approach introduces significant operational risk through private key dependency.

Both methods mint ERC-20 tokens representing proportional vault shares. These shares appreciate or depreciate based on HLP vault performance, creating yield-accruing tokens that track HLP's PnL.

4.2 Depeg Risk Analysis

The primary risk for tokenized HLP other than the native HLP risks is a potential depeg event where the derivative's market value diverges significantly from its underlying HLP vault value. Such divergence typically means that the tokenized version is trading at a discount to its NAV (Net Asset Value), potentially triggering cascading sell pressure and eroding user confidence.

4.2.1 Smart Contract Exploits

Contract vulnerabilities could compromise the backing guarantee through attack vectors such as:

- Excessive token minting without corresponding deposits
- Miscalculation of share ratios during deposits/withdrawals
- Reentrancy attacks during redemption processes

While manually operated HLP tokens maintain relative simplicity reducing attack surface, their immaturity increases exploit probability. The anticipated contract upgrades following CoreWriter's mainnet release introduce additional risk, as historical data shows most smart contract exploits occur post-upgrade. This risk vector affects both tokenization methods equally.

4.2.2 Private Key Compromise

For manually operated tokens, the single EOA controlling all deposited funds represents the most severe risk concentration. Key compromise would grant attackers:

- Complete access to the entire deposited USDC
- Ability to drain funds instantly without on-chain safeguards
- Power to manipulate backing ratios

This centralized control point creates a unique vulnerability absent in CoreWriter-based implementations. The risk severity is extreme with probability of total loss of backing assets, meanwhile the detectability of such compromise remains low until after the exploit has occurred.

4.2.3 Market-Driven Selloffs

Historical events have shown HLP's susceptibility to large-scale withdrawals (70% TVL drop post-JELLY incident). For tokenized versions, this risk amplifies through:

- **Liquidity fragmentation:** Multiple tokenized HLP versions dilute available liquidity
- **Redemption friction:** The 4-day HLP lock-up creates arbitrage opportunities during stress events
- **Cascade effects:** Initial depegs can trigger excess selling and liquidations

During the March 2025 withdrawal wave, a properly functioning tokenized HLP would need to process redemptions while maintaining peg stability, which might be hard to achieve with smart contract limitations on withdrawal rates.

5 Oracle Recommendation

Push-based oracles are optimal for Lending protocols on HyperEVM, providing automated price updates without requiring manual triggers or external intervention. Given the unique risks associated with HLP's market-making strategy and historical vulnerability to manipulation attacks, a multi-layered oracle approach is essential to detect anomalies and prevent depeg events from causing bad debt on the protocol.

5.1 Recommended Configuration

Since each protocol will launch their tokenized HLP token at different times all of them would need a separate price feed to account for the yield generated since the launch. A dual-oracle setup is recommended to provide comprehensive coverage and early warning capabilities:

- **Primary Oracle: Redstone Push-Based Feed**
  - Redstone's tokenized HLP price feeds for direct on-chain pricing using DEXes as primary sources
  - Push-based architecture ensures timely updates without manual intervention
- **Secondary Oracle: Real-Time API-Derived Feed**
  - Direct integration with Hyperliquid's `vaultDetails` API endpoint
  - Calculates live NAV using `accountValueHistory` and portfolio data

  - Display on protocol dashboard for immediate anomaly detection and comparison to the on-chain oracle price
  - Enables rapid identification of HLP vault exploits or manipulation attempts as it bypasses on-chain requirements

5.2 Risk Mitigation Framework

- **Price Deviation Monitoring:** Compare both oracle sources continuously. Deviations exceeding 2% between any two sources should trigger investigations. Deviations >5% should halt new borrows immediately until resolution.
- **Circuit Breakers:** Implement automatic pause mechanisms when API-derived pricing detects anomalous HLP vault behavior, such as sudden PnL swings >10% within short timeframes (< 4H).