One of the core characteristics of AMM deposit receipts (commonly referred to as LP tokens) is that their value is inherently less volatile than the combined volatility of the underlying tokens, thanks to automated rebalancing. This phenomenon, as discussed in @AndreaC 's research piece, positions LP tokens as safer collateral options for lending markets compared to holding the underlying tokens individually.

For LP tokens to be adopted in lending protocols, a price oracle resilient to manipulation is critical. Specifically, the oracle must guard against two key types of attacks:

1. Short-term over-reporting of value

: This could enable attackers to borrow excessive amounts of debt against artificially inflated collateral, resulting in unrecoverable losses during liquidation.

1. Short-term under-reporting of value

: This could allow attackers to trigger liquidations of valid collateral to exploit liquidation penalties, often up to 20% of the collateral's value.

Historically, a significant challenge in using AMM LP tokens as collateral lies in their susceptibility to manipulation within price oracles. Even when robust oracles exist for the underlying tokens, permissionless rebalancing allows attackers to trade against the AMM pool, skewing the marginal price to create "out-of-market" valuations.

Example of a Manipulation Attack

Consider an AMM pool with 1 ETH and 3000 USDC, supported by resilient price oracles reporting ETH at $3000 and USDC at $1. The total market capitalization of the LP token should be $6000 (the product of balances and oracle prices). However, an attacker could, within a single block, manipulate the pool by trading 0.9 ETH for 27,000 USDC, causing the oracle to report a market capitalization of $30,300.

While some AMMs, such as Uniswap, mitigate such manipulation through time-weighted average price (TWAP) oracles, CoW AMMs are by design less vulnerable. This is due to their rebalancing mechanism, which requires bonded solvers to execute trades. However, given the potential very high damage inflicted by borrowing against overvalued collateral, relying solely on solver bonds may not be sufficient.

Proposed Solution

Building on insights from the development of CoW AMMs (in particular their "helper" contracts for widespread solver adoption), we propose a novel manipulation-resilient oracle design. > Specifically, we can compute the "rebalancing trade" that a zero-fee constant function

AMM would accept based on its current balances and external price feeds for the underlying tokens. This allows us to counteract manipulation by simulating the pool's state post-rebalancing.

For instance, even if the manipulated pool balances are 0.1 ETH and 30,000 USDC, we can calculate the hypothetical trade required to restore balance based on the invariant and underlying oracle prices ($3000 for ETH and $1 for USDC). By performing this "counterfactual" trade, we determine the adjusted balances (1 ETH and 3000 USDC) and accurately compute the LP token's true market capitalization of $6000.

This is achieved through the following equations:

1. Ensure the ratio of post-trade balances matches the exchange rate from the underlying oracles:

2. Preserve the constant product invariant:

By solving for R_x and R_y we calculate the rebalancing trade amounts and adjust the LP token valuation accordingly. This method ensures that the LP token's oracle is as robust as the underlying price feeds.

Scope of Work

The grant seeks to implement a manipulation-resilient oracle specifically for CoW AMM pools. The oracle will:

- Adhere to the Chainlink oracle interface.
- Leverage existing Chainlink-compatible oracles for the underlying tokens.
- Support weighted token pools of all configurations.

Deliverables include:

1. A fully functional smart contract implementing the oracle.

2. Comprehensive test coverage demonstrating its resilience to manipulation.

3. Documentation detailing the oracle's functionality and integration, with examples of practical use cases.

This proposal aims to strengthen the security and usability of CoW AMM LP tokens as collateral, enabling broader adoption in lending markets and other DeFi applications.