Concentrated liquidity Market Maker -- KYBERSWAP BUG

The Concentrated Liquidity Market Maker (CLMM) model enhances capital efficiency within a liquidity pool by minimizing slippage. It allows liquidity providers to select their preferred price ranges, thereby increasing their potential yield.

A Concentrated Liquidity Market Maker (CLMM) is a liquidity model that allows liquidity providers (LPs) to allocate their tokens within a selected price range where they will be actively used. Instead of distributing liquidity evenly across an infinite range as in traditional Automated Market Makers (AMMs), CLMMs allow for the pooled funds to be utilized more efficiently within the market or exchange.

Traders can select a specific price range for their tokens, focusing on liquidity where they anticipate market activity. However, using concentrated liquidity market makers (CLMMs) can result in potential losses similar to those associated with active market-making within a traditional order book market.

Users have the ability to take multiple positions for the same token pair, thanks to the flexibility of CLMMs. This allows liquidity providers (LPs) to maximize the effectiveness of the liquidity they supply by establishing various price ranges for their positions.

Ticks

In much the same way that floating point numbers are a discrete subdivision of the infinite real number line, in a CLMM the price range is discretely subdivided into *ticks*. These ticks are denoted by a number but, for a given tick [t], the price at that tick is equal to [1.0001^t]. An LP can provide liquidity between two ticks, as long as the two ticks are an even multiple of the *tick spacing*.

For example, given a tick spacing of 10, an LP could provide a liquidity in the price range $1.00 - $1.22 by depositing liquidity in the tick range (0,2000)(because

```
1.0001^0 = 1.00 and 1.0001^2000 ≈ 1.22
```

KYBERSWAP ATTACK SUMMARY

step 1 : Flash Loan: Borrow 5000 ETH
step 2: Crash the Price: Swap 5000 ETH → USDC
step 3 : Exploit the Bug: Double-add liquidity -- because it lacks the movement check

step 4 : Drain: Buy 6000 ETH for only ~6000 USDC
step 5 : Profit: Return 5000 ETH, keep 1000 ETH

This is check was not applied in past .

```
if (swapData.sqrtP != swapData.nextSqrtP) {
  if (swapData.sqrtP != swapData.startSqrtP) {
    // Only update if price actually moved
    swapData.currentTick = TickMath.getTickAtSqrtRatio(swapData.sqrtP);
  }
  break;
}
```

Problem related to CLMM

There are risks of potential losses if prices move out of the selected range, double counting , frequent funds management, usage of flash loans etc.

CLMM Ai visualizer

[https://claude.ai/public/artifacts/ee6de63d-b93a-456a-8dc7-bb2c1c690786]
