zkSwap Technical Whitepaper - Concentrated Liquidity DEX on zkSync

0xroot, zkWizard, zentoshi

April 14, 2023

Abstract

zkSwap is a highly efficient decentralized exchange that enables traders to swap ERC-20 tokens. It makes use of Concentrated Liquidity to more efficiently distribute liquidity across ranges where liquidity providers expects more price action to happen.

1 Introduction

Automated Market Makers (AMMs) are a form of non-custodial decentralized financial infrastructure that enables trustless financial transactions using immutable algorithms that operate on decentralized ledgers. They have become increasingly popular in the past few years due to the growth of decentralized finance (DeFi). AMMs facilitate the exchange of digital assets such as cryptocurrencies, tokens, and stablecoins, and can be used to create liquidity pools to earn yield from swap transactions.

Recently, DEXs have been gaining traction over their centralised counterparts due to the increased security and privacy they offer. DEXs are powered by distributed ledger technology (DLT) and do not require users to entrust their funds to a third party. This eliminates the risk of potential hacks, which have been a major issue for centralised exchanges. Furthermore, DEXs also offer users greater control over their assets and improved privacy as they are not required to provide personal information when trading. As DEXs are powered by smart contracts, they facilitate trustless transactions, meaning that users do not need to rely on a third party for escrow services. This makes it easier to execute trades quickly and without costly fees. User experience is also getting closer to centralised exchanges day by day, which is driving their adoption and slowly eating up the market share. As a result, DEXs are becoming increasingly popular amongst traders looking for improved security, privacy and control over their funds.

Back then, when the Layer 2 protocols weren't around, the gas efficiency was the main concern when designing a smart contract. DEX concept is introduced into our lives via a simple linear pricing function called Constant Product formula. Its design is so lightweight, simple and efficient that it can run on Ethereum Mainnet without any issues. The formula is used to balance the USD values of the two tokens provided as liquidity. In the next chapter we will be reviewing the formula.

This paper provides an overview of the zkSwap Exchange, an AMM which gives users more control over the price ranges they provide liquidity to and enables a much more efficient trading experience. In the rest of the paper we discuss briefly about the current state of AMMs, including their features, advantages, and challenges. We then explore the concept of concentrated liquidity in detail and provide.

2 Constant Function Market Makers

An AMM is a protocol that relies on a mathematical formula to price assets. Instead of using a traditional order book, assets on AMMs are priced according to an algorithm.Like an order book, however, AMMs use trading pairs – for example, ETH/USDC. The revolutionary part is that instead of having someone on the other side to make a trade, you directly interact with a smart contract. The AMM "makes" the market for you.

One of the most common types of AMM is a Constant Function Market Maker, pioneered by Uniswap. CFMMs work when one type of user, a "liquidity provider," places two assets into a smart contract - creating a "pool" of liquidity. Other users can then trade between those two assets by either depositing and withdrawing from the pool. The price of each of those two assets changes on a fixed "bonding" curve, depending on the ratio of the two assets in the pool. In this way, CFMMs can always make a market, as there will always be some ratio of those two assets with a price determined by the bonding curve.

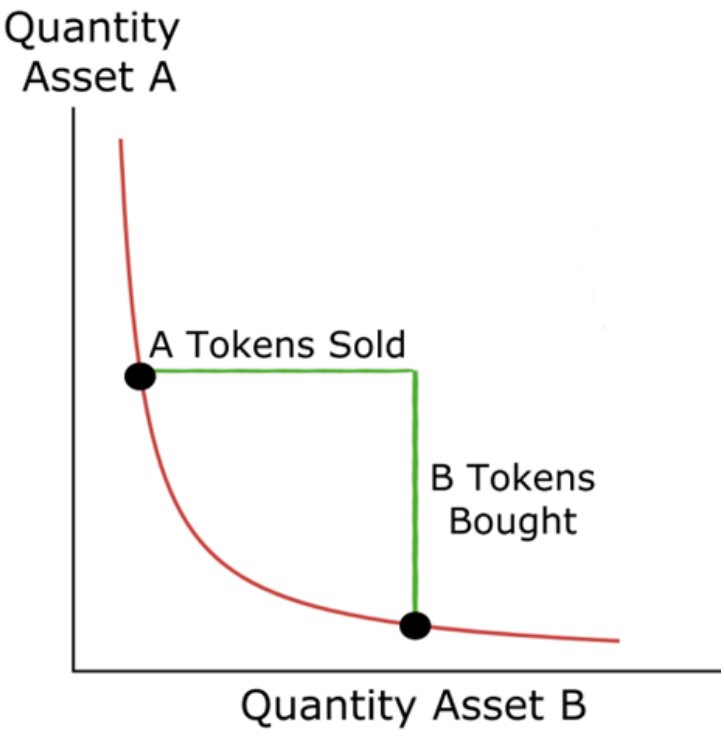
At its core CFMM operates on a very simple mathematical formula:

$$x \times y = k$$

x and y are pool contract reserves–the amounts of tokens it currently holds. k is their product. When traders execute trades, they deposit some quantity of the first token into a pool (the token they intend to sell) and withdraw some quantity of the second token from the pool (the token they intend to purchase). This changes the reserves of the pool, and the Constant Function Formula states that the product of reserves must remain constant. Then the formula for pricing becomes:

$$(x + r\Delta x)(y - \Delta y) = k$$

Δx is the amount of x tokens that needs to be provided to the pool in order to get Δy amount of y tokens out while keeping k constant. This linear pricing formula results in a price curve like the following



In CFMM DEXs, all liquidity is provided across the entire price range $(0, \infty)$. This enables liquidity provided to be fungible, meaning that it has the same price range and characteristics for all users.

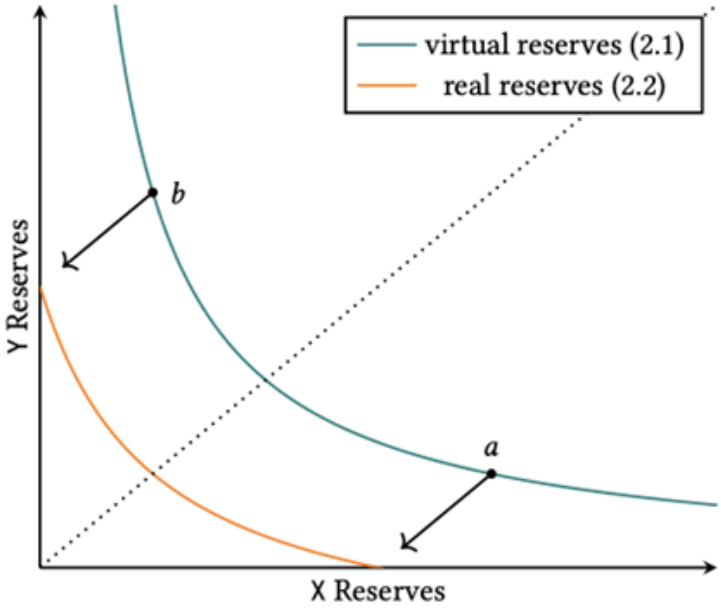
3 CONCENTRATED LIQUIDITY

Although CFMM's simplicity provided gas efficiency, it quickly became obvious that providing liquidity to ranges where price action has infinitesimal probability of happening is not the best use of capital. Following this train of thought, it is logical to enable Liquidity Providers to "concentrate" their liquidity around custom ranges - hence the term "Concentrated Liquidity"

For concentrated liquidity the constant function formula now extends into:

$$\left(x + \frac{L}{\sqrt{p_{\max}}}\right)(y + L \cdot \sqrt{p_{\min}}) = L^2$$

where $p_{\max}$ is the upper range, $p_{\min}$ is the lower range and L is the square root of k. This represents the liquidity of a position that is in between $p_{\max}$ and $p_{\min}$ price levels. The position behaves exactly as a regular constant product AMM in between these two price levels with one caveat; CFMM never touches 0 in each direction however in Concentrated Liquidity formula, when price reaches either one of the ranges, the reserve is fully converted to one of the assets hence making the other asset's price 0. This can be thought of as the usual pricing curve being offset as shown in the following picture



Now with each user being able to set custom ranges, liquidity cannot be represented in a fungible way. Each of the liquidity positions became unique and thus better represented with NFTs rather than ERC20 tokens. The pools now constituted the aggregate of all liquidity positions created by all users.

4 Capital Efficiency

Theoretical Efficiency between a DEX that operates on the regular constant product formula vs a concentrated liquidity DEX can be calculated with the following formula:

$$\frac{2}{1-\sqrt{a/b}}$$

where a and b are the respective price ranges. Let's see an example of this formula in action:

Concentrated Liquidity formula

$$\frac{\text{liquidity}}{\sqrt{\text{lower}}} - \frac{\text{liquidity}}{\sqrt{\text{upper}}}$$

*Lower and upper being upper and lower price levels

If we set liquidity to 1 the equation becomes:

$$\frac{1}{\sqrt{\text{lower}}} - \frac{1}{\sqrt{\text{upper}}}$$

So, we have:

- **V2:** $x \times y = k$
- **V3:** $\frac{1}{\sqrt{\text{lower}}} - \frac{1}{\sqrt{\text{upper}}}$

Let's take the minimum possible price increment called tick for the comparison of capital efficiency $(1, 1.00020001)$

Upper: 1.00020001

Lower: 1

In a Constant Product DEX, with a pool seeded with 1 X and 1 Y tokens, we need to swap exactly 0.000099990001 X tokens. Here are the state changes that occur with swap:

	X	Y	k	Price of 1 X in terms of Y
State 1	1	1	1	1
Change	0.000099990001	0,0001		
State 2	0,99990001	1,0001		1,00020001

Total liquidity of the above pool can be represented (in terms of Y) as

Constant Product: $1\ X + 1\ Y = 1 \times$ price of $X + 1 = 1 \times 1 + 1 = 2$

CLMM: $0.000099990001\ X \times$ price of $X = 0.000099990001 \times 1 = 0.000099990001$

It turns out that the capital efficiency of providing liquidity in the tick range $(0, 2)$ on a concentrated liquidity DEX is $2/0.000099990001 = 20,002$ times more efficient than providing liquidity in the price range $(0, \infty)$ on a DEX with a constant product curve.

5 Auto-compounding Fees and Reinvestment Curve

While most of the CFMMs implement auto-compounding of trading fees into liquidity positions, CLMMs don't have this feature and users have to manually claim the fees. This creates friction as it would be much more efficient to start earning fees from the fees right away. However it is not very straightforward to implement fee auto-compounding into CLMMs due to the unique

nature of liquidity positions. The issue arises when deciding to which price range the fees should be auto-compounded.

First solution that comes to mind would be to provide the fees as liquidity to the same range of the original liquidity position. However the original liquidity position may be out of range at the moment of re-investment. If the position re-invested was out of range, the fees re-invested wouldn't be able to start earning. This would result in a direct loss for the user as it was less costly to leave the fees unclaimed.

In zkSwap, fees are automatically re-invested into a separate curve that essentially acts as a regular CFMM. With this method, we can leverage the fungible nature of CFMMs in the background. To represent the share in the CFMM curve, users are issued a separate ERC20 Liquidity Provider token on top of the NFT that represents their Concentrated Liquidity. The fees invested will start to earn right away regardless of the current price. The total liquidity of a pool can be seen as an aggregation of both curves.

6 Flexible Fees

zkSwap provides various fee structures for the establishment of liquidity pools. Liquidity Providers (LPs) can opt to implement lower fees for trading pairs with reduced volatility to stimulate greater trading activity, or they may select higher fees for pairs that are expected to be highly volatile in order to recompense for risk incurred.

Ultimately, it is anticipated that LPs and Traders alike will arrive at certain fee levels for specific pairs dependent on the features of the underlying tokens and the price movements observed.

7 Farming Rewards

Unique nature of liquidity positions in concentrated liquidity DEXs make it no longer possible to distribute conventional liquidity mining rewards pro-rata via LP shares. In CFMM, all liquidity is equally used thus it's relatively easier to distribute rewards. In CLMM, each user's contribution to the liquidity pool is different. Also the liquidity may be out of range therefore not contributing to price discovery. If left unchecked, this can be manipulated by malicious users by deploying liquidity to safe ranges and farming all the rewards in expense of LPs who actually take on impermanent loss risk.

We need a new mechanism to properly account for the risk taken by each user. Real contribution of users to the price discovery in the pool they have invested in can be measured by the total time the liquidity position has been in range and supporting the current price of the pool. Once the current price leaves the ranges of the liquidity position, the position stops accruing liquidity mining rewards. This simple yet efficient method solves the mercenary farming issue mentioned above and ensures the risk taken by the users are properly compensated by the rewards.

8 Future Improvements

Blockchains today are very similar to the early days of the Internet. There is innovation going on all fronts and the underlying technology has the potential to disrupt every area of our lives. Although it has been 14 years since the Genesis Bitcoin block was mined, the technology itself had limited use cases other than payments. Only in the last couple of years, we started to see blockchain technology being applied as a solution to tangible, real-world problems.

We strive for a future where money and finance is freed from the reign of power groups and are instead a global public infrastructure where all people can have democratized access to. We

believe it is still very early and everything we do can be considered an experiment. Even DEXs are currently considered a financial primitive and relatively "matured" are still very much open to innovation on multiple fronts.

zkSwap Team is actively researching ways to improve the tech and UX for Traders and Liquidity Providers. We present below some areas of research the team is currently working on.

8.1 Dynamic Fees

One of the biggest issues faced by Liquidity Providers is impermanent loss. There has been a lot of discussions around the real PnL for liquidity provision and how most of the LPs are losing money over time, be it CFMM or CLMM. Impermanent loss can be likened to adverse selection in traditional market making, where the MM is left with an unwanted exposure after a sudden market movement.

Traditional market makers use bid-ask spreads to combat market volatility. The bid-ask spread is the difference between the highest price that a market maker is willing to pay for a security (bid price) and the lowest price at which the market maker is willing to sell the same security (ask price). Market makers will use the bid-ask spread to mitigate their risk of loss by setting the difference between the two prices wide enough to cover any potential losses that may occur when the market price of the security fluctuates. By making the spread wide enough, market makers are able to provide liquidity to the market while still protecting themselves against downside risk.

MMs have a lot more ways to combat adverse selection. They combine their market making operations with sophisticated hedging strategies to mitigate risk and try to stay completely market neutral. They also use bid-ask spreads to account for the risk they take in volatile markets. Currently LPs can hedge their risk from external derivatives protocols however playing with bid-ask spreads is not possible.

This simple yet effective tactic can be used to combat volatility in DEXs as well. This can be done on an individual position basis or automatically adjusted for the whole pool based on some kind of volatility oracle. zkSwap Team is researching the best way to make this possible for their LPs.

With the introduction of dynamic fees, one would expect a lot of liquidity to be sucked into the pool as it would offer a much better overall PnL for the users. Increased TVL would reduce slippage thus attracting even more trading volume, feeding the flywheel.

8.2 Farming Automation

Currently staked NFTs need to be rolled over for the next round of rewards manually. If left untouched, the staked NFTs stop earning any rewards. This creates friction for both the users and the zkSwap Team as the zkSwap Team has to manually set new farming contracts each round.

We are researching ways to improve the UX around farming. Off-chain keeper bots could be a solution for this moving forward.

References

https://docs.kyberswap.com/files/Dynamic_Market_Making_v2_whitepaper.pdf

https://uniswapv3book.com/docs/introduction/constant-function-market-maker/

https://uniswap.org/whitepaper-v3.pdf