LUCKYSWAP

luckyswap.finance@gmail.com

January 2021

Automated Market Makers allow digital assets to be traded without permission and automatically by using liquidity pools instead of a traditional market of buyers and sellers. On a traditional exchange platform, buyers and sellers offer up different prices for an asset. When other users find a listed price to be acceptable, they execute a trade and that price becomes the asset's market price. Stocks, gold, real estate, and most other assets rely on this traditional market structure for trading. However, AMMs have a different approach to trading assets.

Since the EVM now gives a gas refund when freeing contract storage or destroying child contracts, one can "bank" their gas by e.g. creating many dummy child contracts, then destroying them when making their desired expensive message call. Gastokens are a class of ERC20 tokens that encapsulate that action inside their token mint and token burn functions. The fact that minting can take place at any time - preferably during the network's downtime with low overall gas price & overall transaction count - and does not need to be confirmed quickly further enables the developer to mitigate the impact of gas fee fluctuation through good planning. GasLucky Token by Luckyswap exchange is currently the most efficient actively-used Gastoken.

Oracle Marketplace is a dedicated decentralized turnkey platform that will connect third parties and exchange important data autonomously. It allows oracle providers to advertise their services and clients the ability to create RFQ's.

Cross-chain solutions are increasingly catching the attention of speculators within the decentralized finance ecosystem. As products and platforms grow in popularity, interoperability between separate chains is becoming increasingly important.

1 Introduction

Automated Market Makers (AMMs) are part of the decentralized finance (DeFi) ecosystem. They allow digital assets to be traded in a permissionless and automatic way by using liquidity pools rather than a traditional market of buyers and sellers. AMM users supply liquidity pools with crypto tokens, whose prices are determined by a constant mathematical formula. Liquidity pools can be optimized for different purposes and are proving to be an important instrument in the DeFi ecosystem.

2. Liquidity Providers

Liquidity refers to how easily one asset can be converted into another asset. Before AMMs came into play, liquidity was a challenge for decentralized exchanges on Ethereum. As a new technology with a complicated interface, the number of buyers and sellers was small, which meant it was difficult to find enough people willing to trade on a regular basis. AMMs fix this problem of limited liquidity by creating liquidity pools and offering liquidity providers the incentive to supply these pools with assets. The more assets in a pool and the more liquidity the pool has, the easier trading becomes on decentralized exchanges.

On AMM platforms, instead of trading between buyers and sellers, users trade against a pool of tokens — a liquidity pool. At its core, a liquidity pool is a shared pot of tokens. Users supply liquidity pools with tokens and the price of the tokens in the pool is determined by a mathematical formula. By tweaking the formula, liquidity pools can be optimized for different purposes.

Anyone with an internet connection and some ERC-20 tokens can become a liquidity provider by supplying tokens to an AMM's liquidity pool. Liquidity providers normally earn a fee for providing tokens to the pool. This fee is paid by traders who interact with the liquidity pool. Recently, liquidity providers have also been able to earn yield in the form of project tokens through what is known as "yield farming."

3. Original definition

AMMs have become a primary way to trade assets in the DeFi ecosystem, and it all began with a blog post about "on-chain market makers" by Ethereum founder Vitalik Buterin. The secret ingredient of AMMs is a simple mathematical formula that can take many forms. The most common one was proposed by Vitalik as:

tokenA_balance(p) * tokenB_balance(p) = k

and popularized by Uniswap as: x * y = k

The constant, represented by "k" means there is a constant balance of assets that determines the price of tokens in a liquidity pool. For example, if an AMM has ETH and BTC, two volatile assets, every time ETH is bought, the price of ETH goes up as there is less ETH in the pool than before the purchase. Conversely, the price of BTC goes down as there is more BTC in the pool. The pool stays in constant balance, where the total value of ETH in the pool will always equal the total value of BTC in the pool. Only when new liquidity providers join in will the pool expand in size. Visually, the prices of tokens in an AMM pool follow a curve determined by the formula.

In this constant state of balance, buying one ETH, brings the price of ETH up slightly along

the curve, and selling one ETH brings the price of ETH down slightly along the curve. The opposite happens to the price of BTC in our ETH-BTC pool. It doesn't matter how volatile the price gets, there will eventually be a return to a state of balance that reflects a relatively accurate market price. If the AMM price ventures too far from market prices on other exchanges, the model incentivizes traders to take advantage of the price differences between the AMM and outside crypto exchanges until it is balanced once again.

4. Automated Market Maker Variations

In Vitalik Buterin's original post calling for automated or on-chain money markets, he emphasized that AMMs should not be the only available option for decentralized trading. Instead, there needed to be many ways to trade tokens, since non-AMM exchanges were vital to keeping AMM prices accurate. What he didn't foresee, however, was the development of various approaches to AMMs.

The DeFi ecosystem evolves quickly, but three dominant AMM models have emerged: Uniswap, Curve, and Balancer.

- Uniswap's pioneering technology allows users to create a liquidity pool with any pair of ERC-20 tokens with a 50/50 ratio, and has become the most enduring AMM model on Ethereum.
- Curve specializes in creating liquidity pools of similar assets such as stablecoins, and as a result, offers some of the lowest rates and most efficient trades in the industry while solving the problem of limited liquidity.
- Balancer stretches the limits of Uniswap by allowing users to create dynamic liquidity pools of up to eight different assets in any ratio, thus expanding AMMs' flexibility.

5. How It Works

All existing AMMs use swap fees to earn profits for their liquidity providers. (The swap fees are configurable in Balancer for each pool, whereas Uniswap charges 0.03% and Curve currently charges 0.04% per swap.) Liquidity providers are ultimately compensated via these fees. But if the pricing function significantly misprices the assets in the pool, as might happen after a sudden exogenous price crash, liquidity providers lose potential profit to arbitrageurs who purchase the mispriced assets.

An AMM can thus maximize its profit in one of two ways: maximizing trading fees, or minimizing arbitrageur profits. Luckyswap seeks specifically to pursue the latter strategy: by introducing virtual balances, arbitrageurs are less able to profit on temporarily mispriced pools, leaving more profit for liquidity providers.

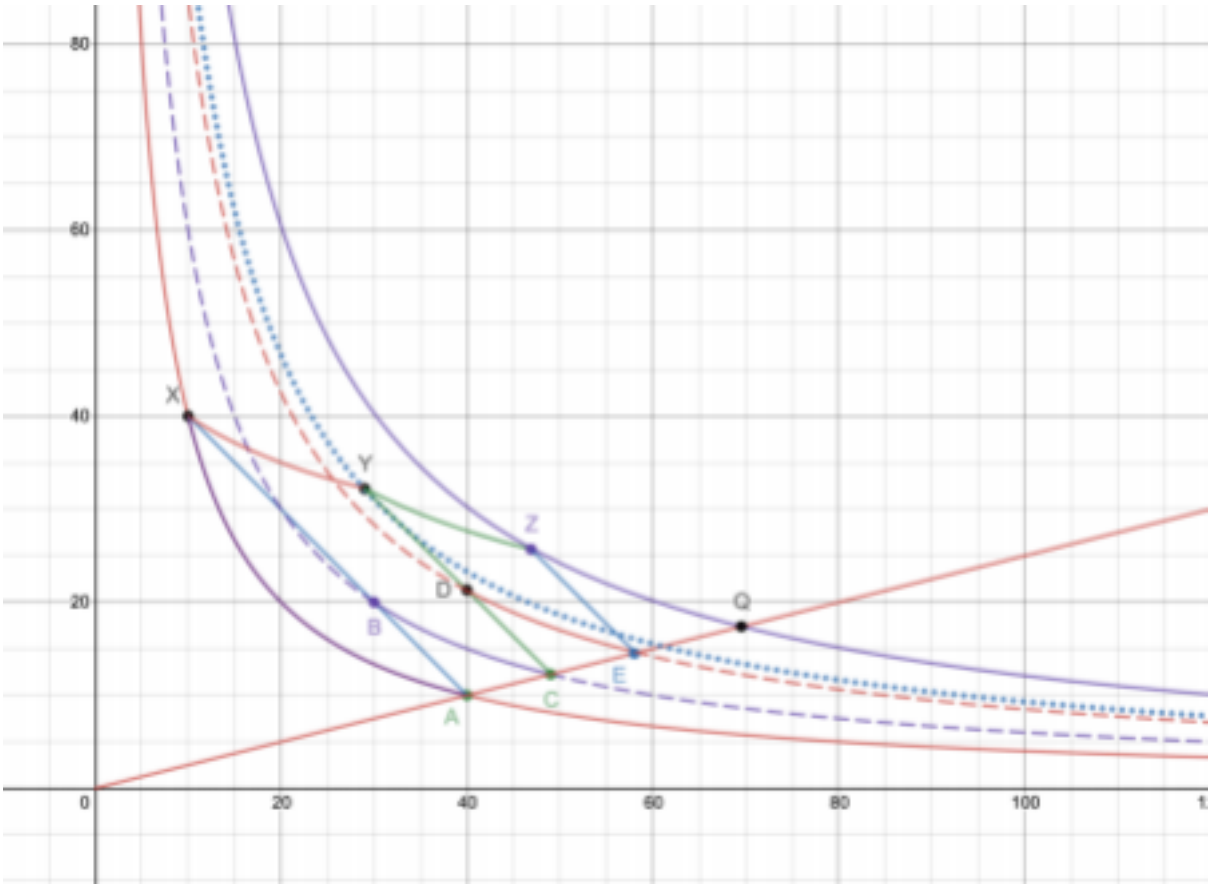
All AMMs with constant product pricing functions offer worse slippage as the trade size increases. Other AMMs instantly provide an arbitrage opportunity in the opposite direction

after a sufficiently large swap (specifically, if the slippage was larger than the protocol trading fee). Arbitrageurs then compete for these arbitrage opportunities by participating in priority gas auctions, paying a significant portion of potential arbitrageur profits to miners. In this model, liquidity providers are not able to capture any of the subsequent profits—aside from the trading fee, all of the revenue from a temporary mispricing is captured by miners and arbitrageurs.

Luckyswap fixes this issue by creating an asymmetry between the two trading directions. Rather than moving both the buy-sell prices simultaneously and offering an immediate arbitrage opportunity, Luckyswap gradually increases the price of the opposite trade. Consequently, the size of the arbitrage opportunity in the opposite direction also increases gradually. This allows the pool to capture some portion of the slippage via further organic trading, rather than giving it all away to the fastest arbitrageur. To achieve that behavior, we have introduced virtual balances that emulate different prices for different swap directions. With virtual balances, purchase of asset A leads the curves for purchasing asset A and asset B to temporarily diverge. The curves eventually converge again over some predetermined time decay. The idea of using virtual balances in AMMs was initially proposed[4] by Vitalik Buterin, to mitigate front-running issues.

6. Mathematical Model

In Luckyswap . when a swap takes place, the pool does not immediately offer a profitable trade in the opposite direction. Instead, it slowly improves the price over some period of time. The following chart shows how several trades would significantly increase the constant-product invariant from point X to point Q.



where A – Initial balances

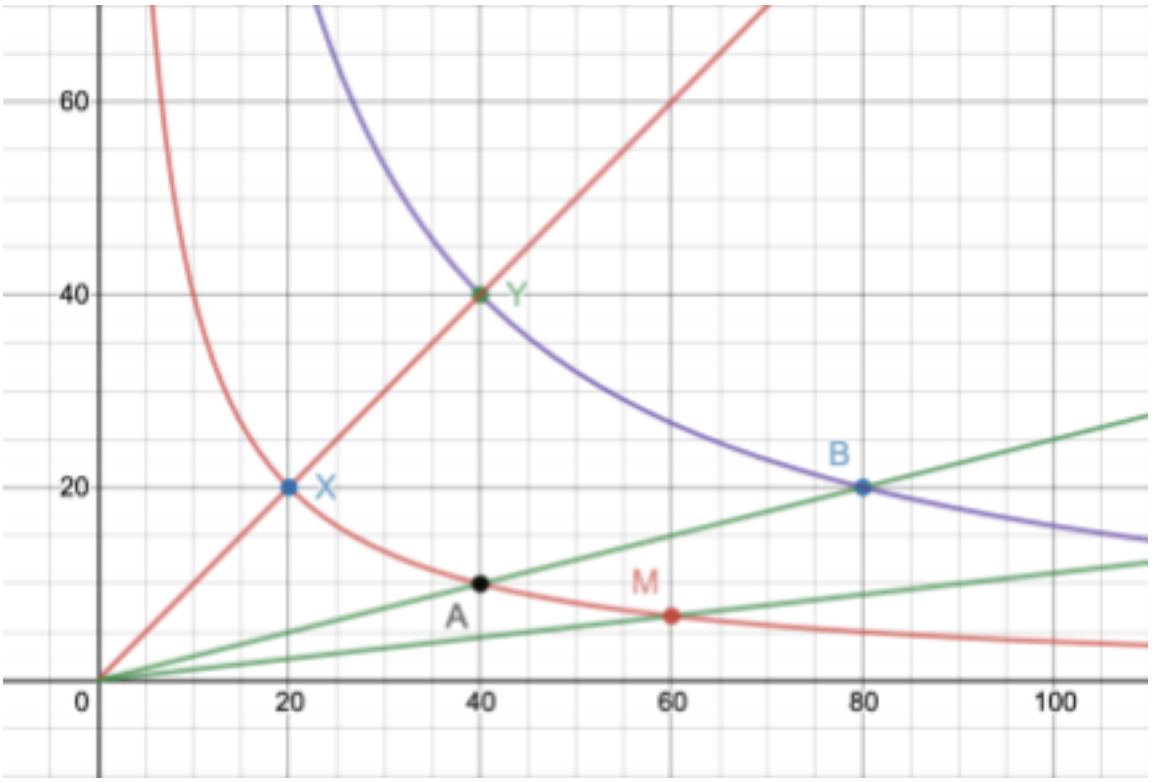
X – Balances after a swap with significant slippage,

B – Virtual balances for the opposite swap after some period of time

After the above swap takes place, the virtual balance for the opposite swap will linearly move from point A to point X. At some point before this full transition takes place, arbitrageurs will attempt to exploit the smaller temporary arbitrage opportunities along the way.

For example, when the virtual balance reaches point B, an arbitrageur may choose to arbitrage the price back to the true price at point C. Note that points A and C (and the origin) are located on the same line, which means they have the same price.

Deposits and withdrawals scale virtual balances in the same proportion as real balances do. The effect of a +100% deposit is shown in the following chart.



where A – Initial real balances,

B – Real balances after deposit,

X, M – Initial virtual balances,

Y, N – Virtual balances after deposit.

Chart 2. Deposits and withdrawals effect on virtual balances (source)

Note that the following equality describes the proportionality between real and virtual balances immediately after deposit or withdrawal:

7. Yield Farming

Actual farmers measure yield as the total amount of a crop that's grown. Accordingly, DeFi proponents have now latched onto the farming metaphor and memed into existence "yield farmers," i.e. folks who measure yield as the amount of interest that's grown atop underlying crypto assets like Dai, USDC, and USDT when put to use in DeFi platforms like Compound, Curve, and Aave

Yield Farming, or the "Agriculture of Yield", is an activity carried out by users (investors, traders) who have assets in cryptocurrencies to use these to invest them and obtain the highest possible return on their investment.

Similar to traditional agriculture, it is carried out in cycles of productivity. The Yield Farmers

look for opportunities in the network to commit their assets in cryptocurrencies to make loans to other users, or to request loans from other users who make a living in the cryptocurrency trade, on the platforms that these offer possibilities. This activity causes more liquidity to occur, and the more liquidity there is in the platform, the greater the number of amounts that can be borrowed.

All ofthis allows Yield Farmers to earn a profit, in the form of interest earned on the amount of cryptocurrency deposited on the platform. And also, in DeFi farmers can receive implicit governance tokens to the platform they are farming. This is part of the earnings received from the high-interest rate proposed by the loan protocol of the platform itself.

Yield farming is closely related to a model called automated market maker (AMM). It typically involves liquidity providers (LPs) and liquidity pools. Let's see how it works.

Liquidity providers deposit funds into a liquidity pool. This pool powers a marketplace where users can lend, borrow, or exchange tokens. The usage of these platforms incurs fees, which are then paid out to liquidity providers according to their share of the liquidity pool. This is the foundation of how an AMM works.

However, the implementations can be vastly different – not to mention that this is a new technology. It's beyond doubt that we're going to see new approaches that improve upon the current implementations.

On top of fees, another incentive to add funds to a liquidity pool could be the distribution of a new token. For example, there may not be a way to buy a token on the open market in any substantial numbers, only small amounts. But liquidity providers can gain access to and accumulate these tokens by providing liquidity to a specific pool.

Yield farming is the practice of staking or locking up cryptocurrencies in order to generate rewards. Many decentralized finance (DeFi) projects rely on yield farming to incentivize users to contribute to the network's liquidity and stability, since these projects do not rely on a centralized market facilitator.

6. Staking Rewards

Staking Rewards is the leading data provider for staking and crypto-growth tools. We are currently tracking 170 yield-bearing assets with an average reward rate of 19.21% and 6725 qualified providers.

8. Governance

Governance is a very important aspect to run a Decentralized Protocol. All developments in the protocol are decided based on the results of the voting. Voting can be done by holders of

the protocol's governance tokens. It is to be noted that though voting is decentralized the there are only a few major whales who hold these governance tokens and therefore take the majority of the decisions. In return for the voting, the voters are rewarded with the Protocol's Governance tokens.

9. Cross Chain

Bridges make Defi cross-functional across blockchains. Using bridges you can transfer tokens from one blockchain to another. Bridges comprise smart contracts that will lock your native token and will give you a 1:1 pegged token for the other blockchain. You can use this pegged token to use in the other blockchain.

10. NFT - Tokenized Version of Digital/Real-world Assets.

A Non-Fungible Token or NFT is a special kind of cryptographic token that represents any unique asset. These NFTs operate as verifiable proofs of authenticity and ownership inside the blockchain network. The NFTs are not interchangeable which introduces scarcity in the digital world of assets.

NFTs are the building blocks of a blockchain-powered or distributed ledger powered world. These NFTs find application in several digital items and processes such as crypto gaming.The notable and first use-case of NFTs in the crypto-collectible trading card gaming.

9.1 What is Fungibility?

The term Fungibility refers to the equal value among the assets. It implies the right to exchange a product or assets with other products or assets of the same kind. These Fungible assets simplify the process of trade and exchange of assets.

Thus any two objects are equivalent in design and their individual units can be replaced mutually is referred to as Fungibility.

9.2 Major Use-cases of NFTs

Let us deeply look at the top use-cases of non fungible tokens in the digital economy. **Gaming**

The most and popular use-cases of Non-fungible tokens is Gaming. Blockchain gaming allows players to securely trade assets and offer a layer of authenticity and verifiability to all the players.

NFTs provides a compelling solution for all digital ownership of game items and allows users to generate real-time revenue by utilizing their gaming skills. Users have the way to decide the direction of future developments within the games.These gives the opportunity to

design their own virtual world & operate in verifiable gaming marketplaces.

11. Oracle Marketplace

As we discussed all the major things about **decentralized finance** which would change the financial system. Definitely, DeFi created a huge hype in the blockchain industry. Also, it has become a recent trend in many platforms

Ether Orders

The smart contract supports trading ether (ETH) for tokens. If the order includes a null takerToken address (0x0) the smart contract will check the value of ether that was sent with the function call and transfer that on behalf of the Taker to the Maker.

Price Oracle

Luckyswap also introduces on-chain volume-weighted average price oracles. Price oracle data is stored as a cumulative sum of all trade inputs and outputs in both directions and it is updated after every transaction. By choosing different periods oracle users can configure the required level of price recency and manipulation resistance. We believe that due to Mooniswap's utilization of virtual balances VWAP oracles will be hard to manipulate by malicious actors.

Conclusion

The Swap protocol serves a growing demand for a decentralized asset exchange on the Ethereum network. Blockchain-based order books, while novel and certainly within the ethos of our ecosystem, have limitations that we believe ultimately make it difficult for them to compete with currently available centralized solutions. Swap provides a method that is both decentralized and unaffected by these limitations.

References

1.https://betterprogramming.pub/what-is-a-blockchain-oracle-f5ccab8dbd72 3.

2.https://medium.com/@ppio/understanding-cross-chain-technology-e36b9c0cfaf3.

3.https://medium.com/ipg-media-lab/the-rise-of-nfts-and-what-it-means-for-marketers 628efc68c90.

4.https://cointelegraph.com/explained/defi-yield-farming-explained