MIP-1
MinSwap - Multi-pool decentralized exchange on Cardano

Long Nguyen
long@minswap.org

April 2021

Abstract

This paper explains the motivations and concepts of MinSwap - an automated market-maker (AMM) decentralized exchange (DEX) on Cardano which supports multiple pricing functions for a single liquidity pool. It also elaborates on the ideas of trade routing, on-chain price oracle and automatic babel fees redemption for Cardano stake pool operators (SPO).

1 Introduction

Traditionally, order-book centralized exchanges have been backed by market makers. Market makers are usually large trading firms or brokerage houses with massive capital, financial knowledge and regulation compliance. They facilitate high liquidity on centralized exchanges and earn profits via the trading spread (difference between buying and selling prices). However, the rise of decentralized exchanges and DeFi has popularized the concept of Automated Market-Making (AMM) which allows individual retailers to easily become market makers and earn profits from trading fees.

On an AMM exchange, individual market makers - now called liquidity providers (LP) pool their funds together to become a single large automated market maker. Traders can trade tokens on these liquidity pools based on a deterministic algorithm. Though being convenient and suitable for on-chain smart contracts, AMM introduces their own classes of problems, namely impermanent loss, low capital efficiency and front-running. These problems are being tackled in different ways by projects on Ethereum blockchains, with different trade-offs. However, no such DEX is being developed on Cardano ecosystem, let

alone an optimized AMM. Having different AMMs for different use cases also confuses non-savvy users and that introduces DEX aggregator such as 1inch [1] or Matcha [6] but they charge additional service fees.

2 Multi-function liquidity pool

By leveraging multiple pricing functions for a single liquidity pool, liquidity providers (LPs) have the option to choose the pool that is most optimized for a specific pair which would yield the highest returns/most capital efficient. At first thought, this might seems to lead to liquidity fragmentation. However, LPs will naturally flow their capital into the most efficient pool for a specific pair because that pool is the most traded against. Automated yield farming strategy created by the community such as the likes of Yearn Finance [8] will also help LPs to re-balance their capital into the most efficient pools. This is no different from having multiple AMM protocols with different pricing functions, but moving liquidity between pools and trading will be faster and cheaper because all pools are on a single platform. Building an AMM with the anticipation for multiple pool functions will also lead to seamless integration of the best ideas from the community without having to do a hard-fork or major migrations.

Let's see what kind of liquidity pool that can be built on MinSwap.

2.1 Constant-product pool

UniSwap [2] popularizes the concept of a constant-product market maker. Constant-product pricing curve works well for most pairs but incurs some impermanent loss for inverse-correlated pairs (i.e. pair that has prices moving in opposite directions). The pricing function on a constant-product pool is really simple:

$$xy = const$$

2.2 Stable pool

Curve [3] has found out that there is a better function for stable pairs (i.e. pair that is similar in price, mostly pegged to an external asset like BTC or USD). It is the combination of constant-product and constant-sum functions with a dynamic "amplification coefficient".

$$An^n \sum x_i + D = ADn^n + \frac{D^{n+1}}{n^n \prod x_i}$$

This helps lower slippage on low-liquidity pools while always ensuring liquidity for large trades.

2.3 Multi-asset pool

Balancer [5] generalizes the concept of constant-product function to more than two assets.

$$\prod x_i^{w_i} = const$$

It allows creating a pool with any amount of any number of assets, instead of limiting the LPs to provide an equal amount of two assets. This basically means that an LP can provide their entire portfolio as it is and get it automatically re-balanced while earning fees.

2.4 Dynamic pool

Kyber extends Curve's "amplification factor" from stable pairs to other pairs in general. The concept is called Dynamic Market Making (DMM) [7]. With DMM, the "amplification factor" is programmed based on a pair's inherent volatility. It also introduces a better fee mechanism where trading fee is adjusted dynamically based on trading volume and price volatility.

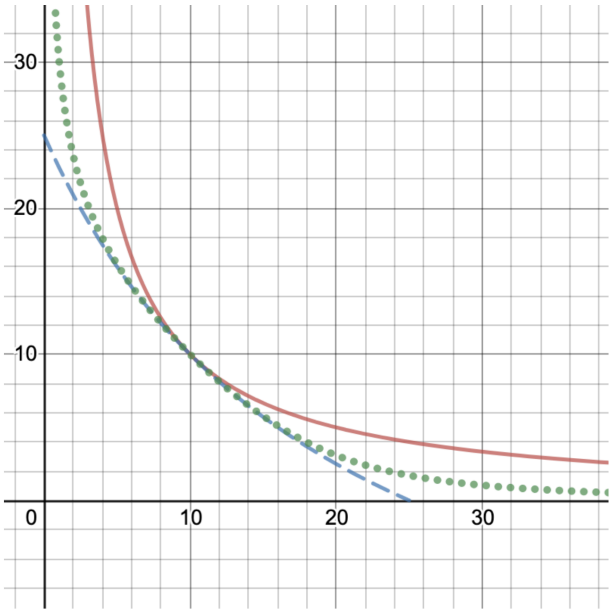

Figure 1: Inventory curves of Uniswap (red), Curve (green) and Dynamic pricing curve (blue)

These four pools are just examples of what MinSwap would be capable of. The AMM space is getting filled with newer and better ideas every day, and the best ideas will get voted by the community to be integrated into MinSwap.

3 Multi-pool routing

With one pair having multiple pools, swapping from token A to token B is not simply executing the constant function on pool(A,B). A simplistic solution to multi-pool routing is finding the pool yielding the highest returns for a specific pair. A better solution could be breaking down the trade size into smaller parts and permuting them to different pools to find the best returns. The multi-pool routing algorithm can be executed entirely on-chain or off-chain as Plutus supports both.

4 On-chain price oracle

One common use case of AMM is to provide on-chain price of a pair without querying and having to trust an off-chain entity. This is made possible because arbitrageur bots will always come in to move the AMM price to market price, as per the law of one price. With the presence of multiple pools for a single pair, the price of a pair will be the weighted mean of all pools for that pair:

$$price(A, B) = \frac{\sum_{i=1}^{n} w_i P_i}{\sum_{i=1}^{n} w_i}$$

where w_i and P_i is the size and price of pool i, respectively.

5 Automatic babel fees redemption

Cardano native assets allow users to pay for a token transaction fee in that exact token instead of in ADA. This concept is called babel fees [4]. It brings better user experience as they don't have to always hold a small amount of ADA just to facilitate token transactions. However, the fee in native token is paid directly to stake pool operators (SPO) and it might cause slow transaction if the token is unpopular and very few SPOs want to be paid in that token. MinSwap will help by allowing SPOs to quickly swap said token into ADA, thus incentivizing SPOs to process native token transactions.

References

[1] *1inch*. URL: `https://1inch.io/`.

[2] Hayden Adams, Noah Zinsmeister, and Dan Robinson. *Uniswap v2 Core*. 2020. URL: `https://uniswap.org/whitepaper.pdf`.

[3] Michael Egorov. *StableSwap - efficient mechanism for Stablecoin liquidity*. 2019. URL: `https://curve.fi/files/stableswap-paper.pdf`.

[4] Prof. Aggelos Kiayias. *Babel fees - denominating transaction costs in native tokens*. URL: `https://iohk.io/en/blog/posts/2021/02/25/babel-fees/`.

[5] Fernando Martinelli and Nikolai Mushegian. *A non-custodial portfolio manager, liquidity provider, and price sensor*. 2019. URL: `https://balancer.finance/whitepaper/`.

[6] *Matcha*. URL: `https://matcha.xyz/`.

[7] Andrew Nguyen, Loi Luu, and Ming Ng. *Dynamic Automated Market Making*. 2021. URL: https://files.kyber.network/DMM-Feb21.pdf.

[8] *Yearn Finance*. URL: https://yearn.finance/.

Disclaimer

This paper is for general information purposes only. It does not constitute investment advice or a recommendation or solicitation to buy or sell any investment and should not be used in the evaluation of the merits of making any investment decision. It should not be relied upon for accounting, legal or tax advice or investment recommendations. This paper reflects current opinions of the authors and is not made on behalf of Minswap Labs or their affiliates and does not necessarily reflect the opinions of Minswap Labs, their affiliates or individuals associated with them. The opinions reflected herein are subject to change without being updated.