Midaswap

V1 WHITEPAPER

ABSTRACT

This paper presents Midaswap, an innovative NFT decentralized exchange protocol. It unifies the reusable concentrated liquidity and the one-off liquidity by having the novel discretized concentrated liquidity mechanism as automated market maker (AMM) and the support for limit orders built in the AMM. Traders will benefit from both the liquidity efficiency provided by concentrated liquidity and the flexibility of limit orders. Midaswap can be implemented under Ethereum Virtual Machine environment.

Martin Zhao

laubswind@midaswap.org

X: @laubswind

October 2023

1 INTRODUCTION

The beginning of decentralized exchanges (DEX) can be dated back to November 2018 when Uniswap first launched. The development of DEXs is based on the development of automated market maker (AMM) mechanism, which uses reserves of assets as parameters in math formulas to describe price curves. The reserves are provided by liquidity providers (LPs) and function as the counterparty of incoming traders. The most classical AMM design is the constant product formula $x \cdot y = k,$ where x and y are reserves of the two assets. During a swap, the k will keep constant and Δx and Δy can be directly calculated. Gradually, the low liquidity efficiency of the classical constant product model pushed people to make improvements based on it. For examples, Curve utilized a more advanced math formula to concisely fit the stable coin pools, and Uniswap V3 [1] introduced concentrated liquidity that allows LP to customize the price range of their positions.

In current Defi market, there are many well-developed AMM solutions for the trading of fungible tokens (FTs) including protocols mentioned above. However, these solutions cannot be directly applied to non-fungible tokens (NFTs) due to their characteristics of unique and indivisible. As the whole NFT market grows, the demand for mature solutions for NFT AMM continues to increase.

In NFT market, NFTX and Sudoswap both provide great NFT AMM solutions from two perspectives. NFTX first proposed the idea of fractional NFT, which breaks NFTs into ERC20 assets, but this approach disregards the differences in NFT IDs and rarities. Sudoswap introduced the Bonding curve algorithm. The Bonding curve requires continuously creating pools to provide liquidity. As a result, liquidity is scattered across different pools, and even within the same pool, it cannot distinguish NFTs' rarities and IDs. In Midaswap, we want to unify the advantages of current AMM solutions and provide better experience for LPs, traders, and even NFT creators.

In this paper, we present Midaswap (v1), a novel NFT AMM that provides high liquidity efficiency while solving the unique needs in NFT markets.

2 CONCENTRATED LIQUIDITY

The concept of concentrated liquidity originates from Uniswap v3 [1]. It allows liquidity providers (LPs) to concentrate their liquidity within a customized and arbitrary price range. As implemented in Uniswap v3, it improves the liquidity efficiency and allows LPs to make their own liquidity strategies.

However, the Constant function algorithms used in Uniswap and many other protocols do not fit the trading scenarios of NFTs. Therefore, we introduce the concepts of Liquidity Book & Bin with Discretized Concentrated Liquidity that utilizes Constant sum algorithms locally. It inherits the high liquidity utilization efficiency of Uniswap v3 while reducing contract complexity and saving gas.

2.1 Liquidity Book & Bin

The Discretized Concentrated Liquidity has been previously used in Trader Joe [2] and iZiSwap [3]. To not confuse users, we choose to keep using the terms “Liquidity Book” and “Bin” from Trader Joe.

In Liquidity Book, the liquidity of an asset pair is distributed in discrete price bins. Each bin is a price point, which means that each bin has its own constant corresponding swap rate. A simple example of liquidity distribution could be represented below.

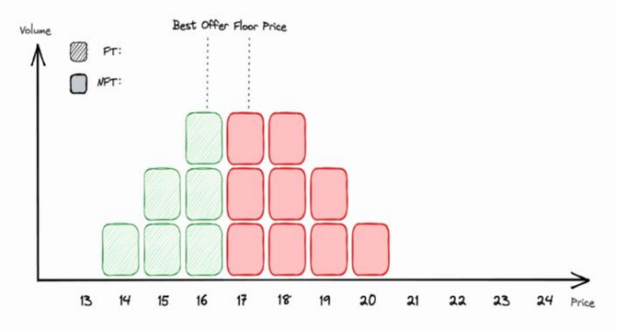

Figure 1: Example Liquidity Distribution

It is worth noting that in the figure above, a box of NFT liquidity represents one NFT, and a box of FT liquidity represents the amount of FTs equal to the price of an NFT in the corresponding bin.

As mentioned above, the swap price of a single NFT depends on the bin where the swap happens. The mathematical relationship between them is straightforward.

$$Price = 1.0001^{BinId - 2^{23}} \tag{2.1}$$

The range of the integer *BinId* is set to [7501336, 9275880], ensuring that the range of *Price* is (2^{-128},2^{128}).

In each bin, the quantitative relationship of base asset (X) and quote asset (Y) can be represented by the equation below, where L is an integer representing the total reserve of a bin and remains unchanged after every swap.

$$x + \frac{y}{Price} = L \tag{2.2}$$

2.2 Range Orders

Liquidity from LPs can be viewed as range orders. LPs need to set the bounds for the liquidity they provide and it is possible that the liquidity does not fill each bin between the bounds.

There are four types of orders that users can place in Midaswap: buy orders, sell orders, limit buy orders, limit sell orders—all of these are in the form of range orders.

Buy orders and sell orders are quite similar to positions in Uniswap v3 [1]. They are two-way orders, so there is no guarantee that LPs will receive the desired asset. LPs bear the risk of impermanent loss and earn LP fees from swaps.

Limit buy orders and limit sell orders are very similar to commonly used limit orders. They are one-way orders, so once the limit orders are filled, the liquidity will become inactive and locked for LPs.

The figure below compares the liquidity distribution of a single position in different designs. In Uniswap V3 [1], the liquidity is uniformly distributed in the chosen price range. In Trader Joe V2 [2], the liquidity is uniformly distributed in all bins in the chosen price range. In Midaswap, the liquidity is uniformly distributed in the chosen bins. It is essential to understand that Midaswap supports the range order by transferring price range into bin sequence through frontend. More details about the “chosen bins” will be discussed in section 4.2.

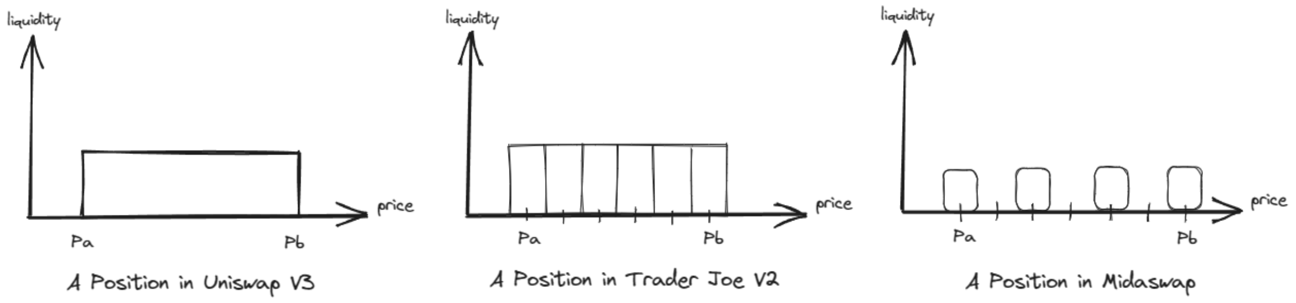

Figure 2: Example Single Position Distribution

3 PROTOCOL ARCHITECTURE

For future Midaswap LPs, it is very important to understand the pricing mechanism and the auto-arbitraging in this section. Features in this section will affect how LPs will make their strategies and take the corresponding risk.

3.1 Pricing Mechanism

Both Bin price Curve and LP price Curve construct the pricing mechanism in Midaswap.

The Bin Price Curve simply uses the x+y =k model, and it tracks liquidity by using binary tree. When traders sell NFTs, the system will find the best offer bin and the corresponding LP, and if the liquidity in the bin is not enough for a swap, the binary tree will help to find the next bin.

The LP price curve is a little bit different. When LPs add liquidity, they need to choose a price range, which, at the contract level, is actually a serious of bins. In each of these bins. one LP owns either a box of FT liquidity or a box NFT liquidity. When an NFT is sold to this LP, the highest FT liquidity box becomes the NFT liquidity box. When a user buys an NFT from this LP, the lowest NFT liquidity box becomes FT liquidity box.

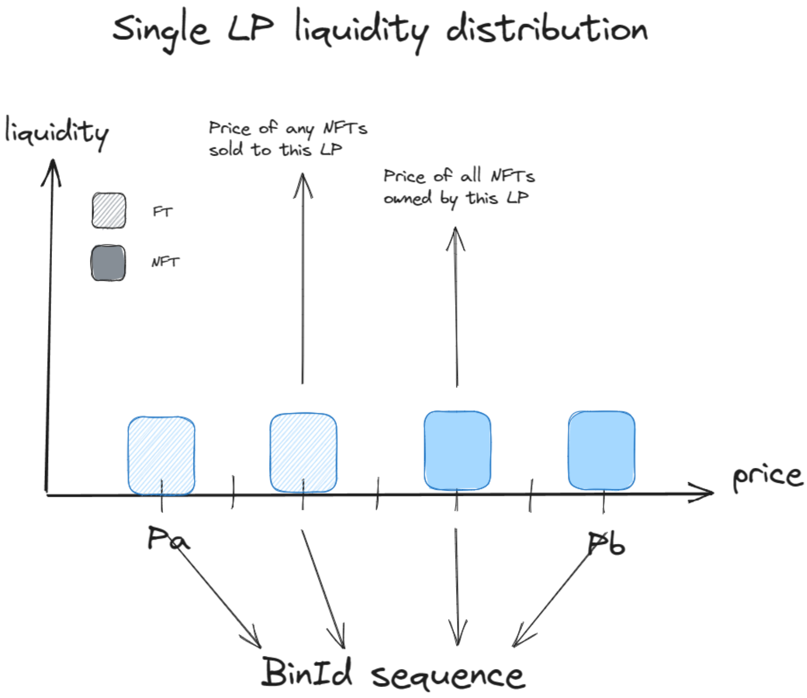
Single LP liquidity distribution
liquidity
Price of any NFTs sold to this LP
Price of all NFTs owned by this LP
FT
NFT
price
Pa
Pb
BinId sequence

Figure 3: Example LP Liquidity Composition

With the LP price Curve, LPs no longer need to price their NFTs one by one; instead, they only need to provide two price range bounds.

This saves time for LPs and also utilizes market to promote NFT trading as much as possible. However, the disadvantage of this mechanism is obvious : the most valuable NFT in a position will get bought first in a relatively low price. Therefore, we discourage LPs from adding NFTs with significant differences in value within a single position and choosing a too wide price range.

The figure below shows how the bin price curve and LP price curve work simultaneously in Midaswap. (colors of liquidity boxes represents LPs)

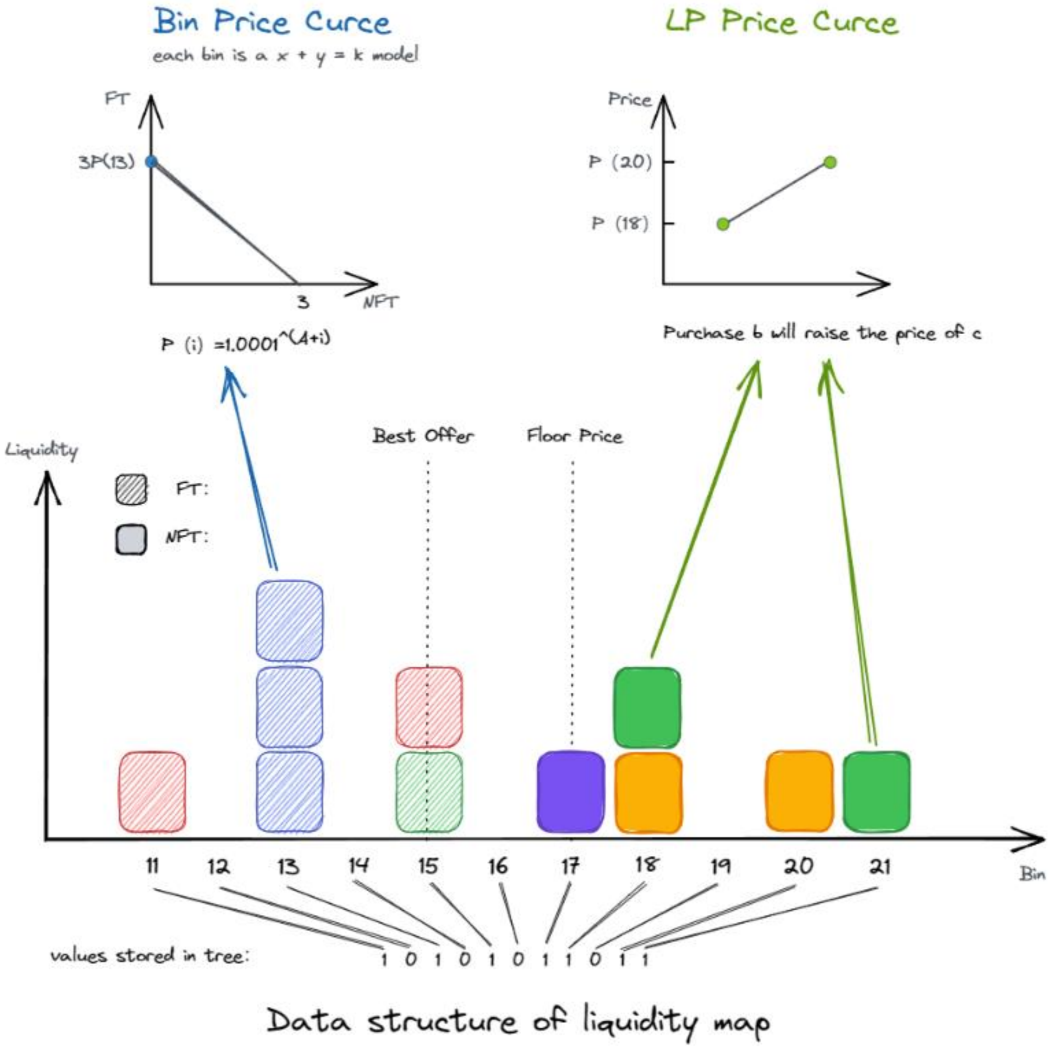

Figure 4: Example Liquidity Map of Different LPs

3.2 Auto-arbitraging

It might be counterintuitive that a trading model has two pricing logics that run at the same time. A small issue under this design is: there is a chance for traders to complete arbitrage within this system. There can be at least two cases:

Case 1: The arbitrager can buy a target NFT A from a two-way liquidity LP and then sell another NFT B to him. We would consider the “value” gap between A and B as the profit of this arbitrage.

Case 2: A user buys a very expensive NFT A from a two-way liquidity LP, and then a box of FT liquidity will appear in a very high bin. At this moment, an arbitrager can buy a floor price NFT B and then sell it in this bin. We would take the price gap between A and B as the profit of this arbitrage.

In either case, the LP who provides liquidity in very high bins will end up receiving floor price NFTs. To solve this problem that most LPs would not like, we introduce the Auto-arbitraging. Auto-arbitraging is a feature that automatically checks the status and arbitrages for the LPs after every swap. Instead of letting LPs be arbitraged, the system chooses to arbitrage first and leave the profit to LPs.

The figure below illustrates the difference that Auto-arbitraging makes after a user buys an expensive NFT.

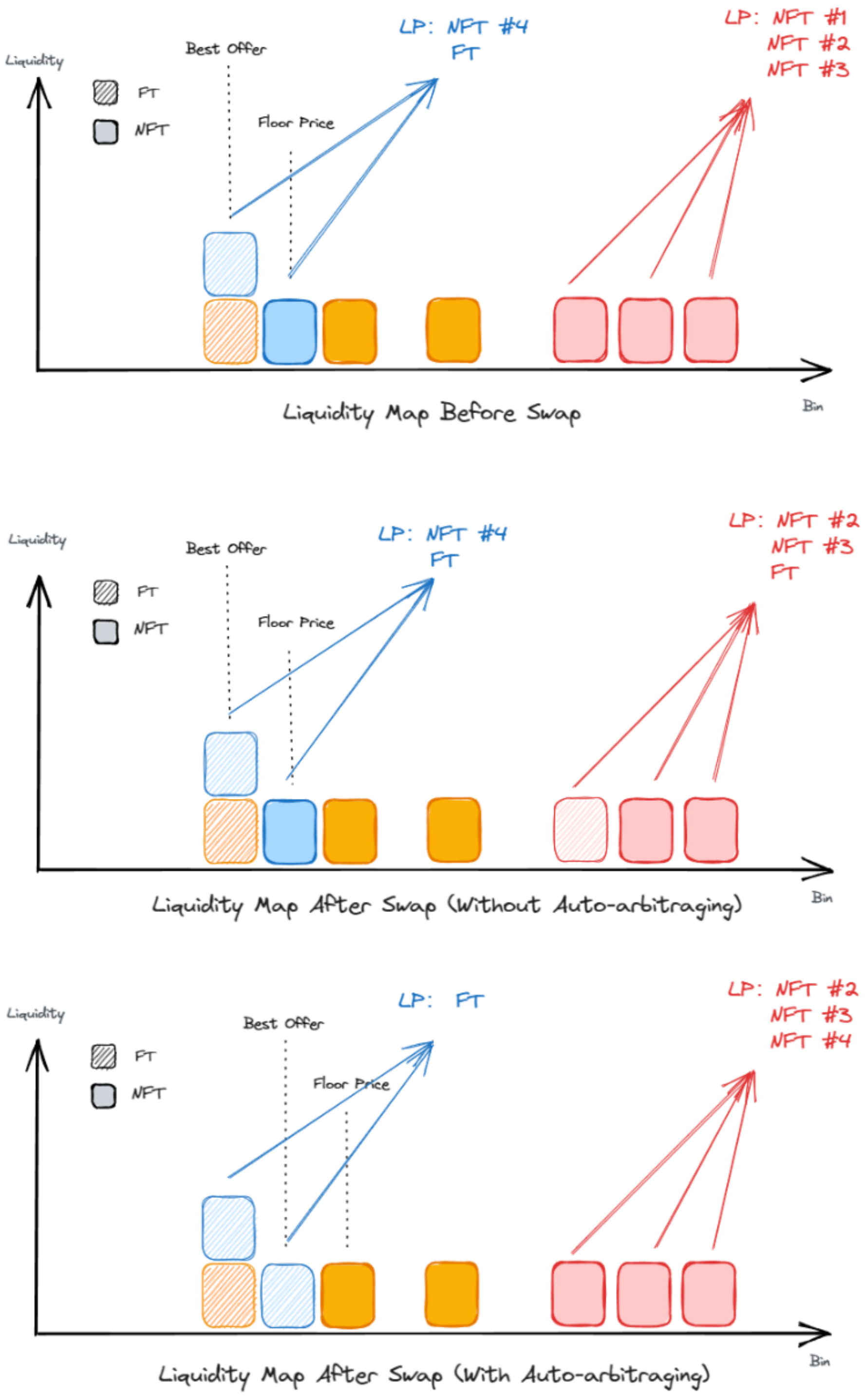

Figure 5: Example Before/After Swap Cases

When a user buys an NFT (the target NFT, NFT #1 in the figure above), the system will find a floor price NFT (NFT #4 in the figure above). The whole purchase process can be viewed as two steps:

- Step 1: The user buys the floor price NFT. Fees will be charged as normal.
- Step 2: The user uses the floor NFT and the price gap between these two NFTs to swap the target NFT. The user gets the target NFT and the red LP owns the floor price NFT and the price gap. No fees will be charged in this step.

4 USER INTERACTION

4.1 Create pools

Midaswap is a permissionless AMM. Anyone can create a pool of an arbitrary pair of FT-NFT. There are a few limitations on creating pairs.

- One pool for one pair. Users cannot create a pair that has already been created.
- Users must add liquidity to activate creating the pool.

4.2 Add/remove liquidity

Positions in Midaswap are range orders (see section 2.2). The liquidity distribution of a position is determined only by a non-decreasing arithmetic sequence of BinIds.

Parameters	Type	Description
LP Token ID	uint128	Position ID. Its parity is used to represent whether the order is limited.
startBin	uint24	The initial term of the arithmetic sequence.
binAmount	uint24	The number of terms of the arithmetic sequence.
binStep	uint24	The common difference of the arithmetic sequence.
lpFees	uint128	The fees earned by the LP, including the price gap paid by auto-arbitraging. It can be claimed or withdrawn.

Table 1: Position-Indexed State

LPs need to provide price bounds and the amount of asset to add liquidity. The frontend will calculate the corresponding arithmetic sequence. The contract will finally record startBin, binAmount and binStep under the LP Token ID.

The LP Token in Midaswap is in the form of ERC-721 due to the non-fungible nature of positions. The protocol supports the query of net value of LP Tokens, so that other protocols can support their compossibility.

4.4 Fees & Swaps

It is important to note that, in Midaswap, all fees are charged in FTs due to the non-fungible nature of NFTs.

Fees in Midaswap includes base fees and royalty fees. Base fee generates income for LPs and royalty fee generates income for NFT creators. Both the base fee and the royalty fee are calculated as portions of total value of traded NFTs. Base fee rate (f_b) is initially set as 0.5% and royalty fee rate (f_r) is set by NFT creators.

We use TV to denote the total value of all NFTs during a single swap.

Base Fees for buying NFTs:

$$F_b = \mathrm{TV} * \mathrm{f_b}$$

Royalty fees for buying NFTs:

$$F_r = \mathrm{TV} * \mathrm{f_r}$$

Base Fees for selling NFTs:

$$F_b = \mathrm{TV} * \frac{1}{1 + \mathrm{f_b} + \mathrm{f_r}} * \mathrm{f_b}$$

Royalty fees for selling NFTs:

$$F_r = \mathrm{TV} * \frac{1}{1 + \mathrm{f_b} + \mathrm{f_r}} * \mathrm{f_r}$$

From the formulas above, we can simply get the amount of FTs that users pay and receive during swaps.

When buying NFTs, users need to pay:

$$\mathrm{amountIn} = \mathrm{TV} * (1 + \mathrm{f_b} + \mathrm{f_r}) \tag{4.1}$$

When selling NFTs, users will get:

$$\mathrm{amountOut} = \mathrm{TV} * \frac{1}{1 + \mathrm{f_b} + \mathrm{f_r}} \tag{4.2}$$

As we have mentioned in this paper, the swap procedures of buying an NFT and selling an NFT are not perfectly symmetric. The figure below describes the control flows of these two actions.

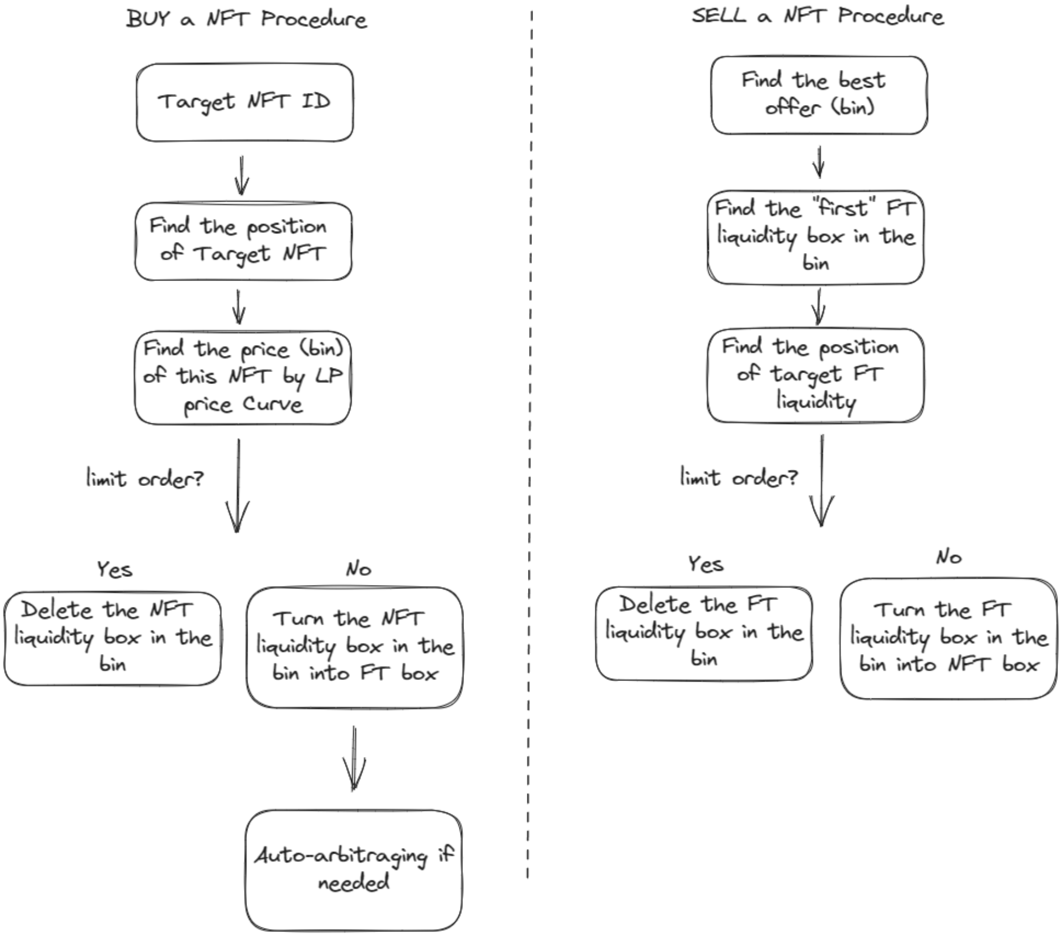
BUY a NFT Procedure
Target NFT ID
Find the position of Target NFT
Find the price (bin) of this NFT by LP price Curve
limit order?
Yes
No
Delete the NFT liquidity box in the bin
Turn the NFT liquidity box in the bin into FT box
Auto-arbitraging if needed
SELL a NFT Procedure
Find the best offer (bin)
Find the "first" FT liquidity box in the bin
Find the position of target FT liquidity
limit order?
Yes
No
Delete the FT liquidity box in the bin
Turn the FT liquidity box in the bin into NFT box

Figure 6: Swap Control Flows

5 ERC-1155

Midaswap is an AMM specially designed for NFTs trading, but not only for NFTs. All of the features and mechanisms we mentioned in this paper are applicable to the ERC-1155.

It is worth noting that although auto-arbitraging can be applied to ERC-1155, but no rational economic actor would buy an ERC-1155 when there is an identical ERC-1155 available at a lower price.". Thus, ERC-1155 buyers are assumed to buy ERC-1155s at floor price.

REFERENCES

[1] H. Adams, N. Zinsmeister, M. Salem, R, Keefer, and D. Robinson. 2021. *Uniswap v3 Core*. Retrieved Sep 20, 2023 from https://uniswap.org/whitepaper.pdf

[2] MountainFarmer, Louis, Hanzo, Wawa, Murloc, Fish. 2022. *Joe V2 Liquidity Book Whitepaper.* Retrieved Sep 20, 2023 from

https://github.com/traderjoe-xyz/LB-Whitepaper

[3] J. Yin and M. Ren. 2021. *iZiSwap : Building Decentralized Exchange with Discretized Concentrated Lliquidity and Limit Order.* Retrieved Sep 20, 2023 from https://assets.izumi.finance/paper/dswap.pdf