WhaleSwap:

Time Weighted Average Market Maker Implementation

WhaleSwap

Executive Summary & Overview

Decentralized finance (DeFi) as a space seeks to replace traditional finance that requires the use of middlemen or centralized parties. Automated Market Makers (AMMs) are part of DeFi in that they replace traditional order book exchanges of buyers and sellers seeking to trade with a digital way to buy and sell digital assets through liquidity pools. That is, the purpose of an AMM is to trade one cryptocurrency asset for another. Users of AMMs provide liquidity through providing crypto tokens, forming liquidity pools. Rather than buyers and sellers determining prices, the decentralized nature of AMMs means that prices are determined by a mathematical formula (x (token 1) y (token 2) = k most commonly) where someone seeking to trade one token for another is essentially trading against a liquidity pool. This pool is provided by users called liquidity providers, suppliers of tokens who earn fees based on the percentage of liquidity they provide when trades occur. In trading against a liquidity pool, one trades against an algorithm called a smart contract. Smart contracts are computer programs on the blockchain that run when conditions are met.

With WhaleSwap, our novel AMM project, we aimed to implement the fundamental functionality of an AMM from scratch having spent an enormous time digging into research and understanding the fundamental concept of creating liquidity pools algorithmically. Then, we aimed to implement the time weighted average market maker (TWAMM) functionality, which allows for easier, more efficient large-volume transactions. WhaleSwap would allow for long term order (LTO) creation, cancellation, and withdrawal. TWAMM is a concept originating from a white paper written by Paradigm, a top investment firm in the crypto space. Essentially, because liquidity pools are finite and price is determined by a constant formula that considers the supply of the tokens, when a large trade, executed by “whale traders” with large amounts of capitals occurs, the price is extremely distorted.

The idea of TWAMM is to have a mechanism by which a sufficiently large transaction is broken down into infinitely many small transactions over a period of time, rather than executing the transaction all at once. The concept also depends on traders looking for arbitrage opportunities to come in during this process when they see the price starting to increase for a token gradually as its supply decreases. There are a lot of moving parts in executing this because it involves optimizing gas fees (the fees paid to miners on the Ethereum blockchain as well which skyrocket when many transactions are performed), challenges with supply limitations,

pooling orders together, and assuming some of the sub-orderders occur between blocks to avoid some malicious trade attacks.

Value Proposition & Need

Our value proposition, on top of the inherent capabilities of an AMM, is to make the execution of large orders more efficient and less price-distorting.

The code for market makers like Uniswap and SushiSwap is open-source, meaning it is available to the public. The key competitive advantage to an AMM firm is the amount of users / traders, and hence trade volume that allows for fee generation. Once users get comfortable with one platform, its rules, and its interface, the switching costs become high, so it can be difficult moving liquidity from one platform to another. Despite the success of existing protocols in the space today, there are inefficiencies and papers, research, and innovative solutions being published regularly. However, existing protocols like Uniswap do not change very much and it is difficult to upgrade them due to their decentralized nature. Thus, integrating the TWAMM functionality into an existing player is difficult. With WhaleSwap, we are implementing the fundamental properties of an AMM while also implementing TWAMM, which currently has not been implemented by any of the top protocols. In essence, we are aiming to take a white paper on a potential concept and allow for smoother, more efficient processing of large transactions in this DeFi space.

Given our goal of diving deep into the fundamental functionality of the AMM, we build the base AMM functionality, such as the constant product formula, and ability to execute basic swaps ourselves and not using the open source code. Of course, we can in the future replace what we have written with existing code and connect it to the TWAMM functionality.

Stakeholders

Traders / users

The success of an AMM depends on users trusting the protocol and using it to actually execute trades. This is how the liquidity providers (LPs) providing the supply of tokens earn income and are motivated to continue providing liquidity as well as how the AMM ultimately earns revenue (through a spread on the fee). There is certainly a first-mover advantage but given more appealing features, such as a more intuitive UI, lower fees, or lower gas fees to miners on

Ethereum, this first-mover advantage deteriorates. Whales, institutions or large controllers of capital, would be key here, given the TWAMM concept.

Liquidity providers / investors

LPs need to be incentivized to provide liquidity in liquidity pools (ie supply tokens that traders can trade against) through the incentive of earning income based on the percentage of the pool they are contributing. That is, these stakeholders need to trust the protocol and AMM infrastructure in that it will likely be an income-generator rather than a source of loss.

Market maker employees

Despite the decentralized nature of an AMM, the team coding the protocol and deploying the contracts is a stakeholder. With Uniswap, this was a small team that created the protocol based on an Ethereum funding grant and later venture capitalists who invested in the company hoping to earn some sort of return.

Government & regulatory figures

As AMMs and DeFi come under increased scrutiny from the government given the billions of dollars being traded in these industries now, there may be risk that the concept or functionality of AMM as a decentralized exchange may come at risk. Ultimately, in WhaleSwap and other AMMs, you are trading against a smart contract algorithm .

Market Opportunity & Customer Segments

The way in which players in the AMM space compete is mainly based on user base size, fee structure (how much users pay per trade), mathematical foundation / architecture for the protocol, and interface / UX. In fact, marketing and branding is a large space for innovation and competition. For example, SushiSwap has an interface and naming convention that is all based on a Japanese sushi restaurant, which adds an element of excitement to the platform.

Decentralized exchange segments are difficult to segment, but Pew Research reported that 3/10 Americans aged 18-29 have invested or traded a cryptocurrency. The most opportunity comes with the gender disparity in usage as 49% of men in this age bracket have done so compared with 19% of women. While older demographics do not seem to be as likely of a target, but still have potential given more transparency and intuition in these mechanisms, young women present a real opportunity.

Estimation of the Size and Growth of the Market Segment

According to Ethereum-based data aggregator Dune Analytics, Decentralized Exchanges (DEXs) have had $1,084B volume traded in the last 12 months as of April 29, 2022. Dune tracks that there are 5,097,826 unique traders on these platforms. With market share defined by 7 days volume, as of April 29, 2022, Uniswap is the leader with $9.9 bn 7 days volume. Uniswap hit $20 bn in monthly volume in February 2021. From 2019 - 2021, cumulative monthly volume on DEXs increased by 1,000%. According to an article from Cointelegraph, the growth in the last year has been unevenly distributed in the space, with AMMs and aggregators (pooling different DeFi services) experiencing the largest growth. There is currently no signs of growth slowing down in this space.

Competition

In the field of decentralized exchanges, (DEXs), some of the biggest players are Uniswap (the original AMM), SushiSwap, and PancakeSwap.

Uniswap

Uniswap is the market leader and has $4.7 bn Total Value Locked (TVL) (Ethereum) as of April as well as about $1.7 bn in 24 -hour trading volume as of this report. Uniswap launched Version 3 in May 2021 as it continues to innovate and try to become not just the first, but most effective AMM. Uniswap is venture-backed and it decided to not release its V3 code openly unlike with the other versions, as there does seem to be some desire for control despite the decentralized goal of an AMM.

SushiSwap

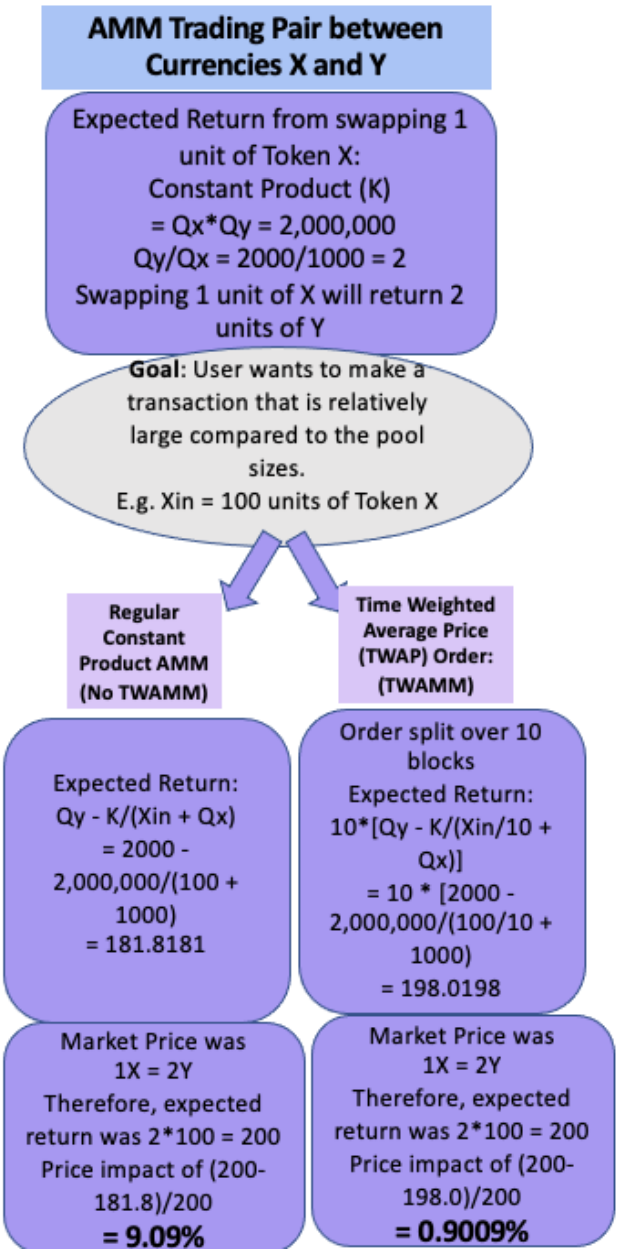
SushiSwap was forked from Uniswap given that the code is open-source, as aforementioned. SushiSwap offers a governance token, SUSHI, which allows those who have it to have voting rights, such as protocol updates, which is a crucial power to hold in a decentralized system. While Uniswap also has UNI as a governance token, SushiSwap has not stopped giving this token out and is therefore, has a reputation of a more community-accessible AMM.

PancakeSwap

PancakeSwap is also a fork from Uniswap, but built on Binance Smart Chain instead of on Ethereum. While Ethereum has first mover advantage, Binance is sometimes considered a faster and cheaper alternative with lower gas fees. PancakeSwap has lower fees for trading and has a

more fun element for users, such as having a daily lottery that chooses winners of governance tokens at random.

To summarize, WhaleSwap differentiates itself from these traditional AMMs in that 1) traditional AMMs have price slippage resistance due to liquidity pool depth while WhaleSwap is aimed to be architected to handle large orders, 2) is more capital efficient and aimed for large-capital traders, and 3) aims to have a more digestible interface. The diagram below summarizes how breaking a large order through the TWAMM concept reduces the price impact:



Cost

The main costs that an AMM creator incurs would be auditing and deploying contracts to mainnet (real blockchain). Since our team is focusing on creating functionality on a test network (testnet), we are not currently incurring these costs. However, far in the future, if we were to deploy to mainnet, auditing a contract can be between $5,000 to $15,000 USD, according to Fintech News. Auditing is primarily for security and is likely crucial. Deployment will be another expense that can be estimated from the gas consumption of deployment on a testnet multiplied by the gas price. It is hard to estimate this but according to an article on Medium, it can be thousands of dollars. Another cost would be supporting the team who would manage this full-time.

Revenue Model

The initial go-to-market strategy for these AMM players has been to put off revenue generation in light of acquiring as large of a base of trade volume and users as possible due to network effects. For example, Uniswap, while receiving venture funding throughout its development, deployed its AMM protocol using grant funding. It was not until its code update, V2, when the company was already trading billions of dollars in volume, that Uniswap introduced a revenue-creating mechanism that they can turn on and off, which includes protocol fees off of transactions. Uniswap has fee tiers that are 0.05%, 0.3%, and 1% depending on the risk of the liquidity. Until V2, all of this went to LPs as profit but Uniswap now can also take a portion of that fee as revenue. That is, Uniswap takes a spread in the fees traders pay to LPs who are providing liquidity. Furthermore, Uniswap issued a token for revenue generation, too.

Given this, one competitive advantage in building an AMM can be defined by the ultimate fee structure. SushiSwap has 0.3% transaction fees, while Pancake has 0.2% transaction fees, making it less expensive for traders. With SushiSwap, 0.25% goes directly to the LPs providing the liquidity, while the rest of the 0.05% goes to SUSHI (governance coin) owners, which is essentially the revenue generation mechanism. Therefore, an assumption that can be made is that were we to deploy this to a mainnet, while our main goal would be to initially get users, our revenue model would be based on the transaction fee spread we charge. Assuming we would certainly not go higher than 0.3% (the current market maximum) and given we would want to incentivize whale traders with large amounts of capital, we could have fees of 0.25%, the

value of which would be justified by efficient handling of large transactions while charging less than Uniswap and SushiSwap. The spread WhaleSwap would take would likely still need to be 0.5% or LPs would not be incentivized to contribute liquidity. The revenue will then be a function of the estimated transaction volume, which is challenging to predict prior to launch and a user base, and the spread.